بسم الله الرحمن الرحيم

هذا الملف الشامل لكتاب الحرب الإلكترونية -الجزء الأول- مع الملحقات يحتوي على التالي:

- كتاب الحرب الإلكترونية الجزء الأول: الأمن السيبراني
- دراسة ملحقة: أفضل خدمات VPN 2023
- دراسة ملحقة: أفضل محاكيات Android
- دراسة ملحقة: أفضل برامج مكافحة الفيروسات لعام 2023
- دراسة ملحقة: ما هو أفضل تطبيق آمن للمراسلة

صادر عن

مؤسسة كتائب الإيمان

جيش الملاحم الإلكتروني

إعداد مجلس التعاون الإعلامي الإسلامي

فهرس المحتويات

الحرب الإلكترونية

الجزء الأول

الأمن السيبراني

تقديم مؤسسة كتائب الإيمان للإنتاج الإعلامي



١٤٤٥ - ٢٠٢٣

بسم الله الرحمن الرحمن

مؤسسة كتائب الإيمان

تقدم

سلسلة الحرب الإلكتروني

*** كتاب الحرب الإلكترونية- الجزء الأول: الأمن السيبراني ***

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

المقدمة

قال الله ﷻ (يَا أَيُّهَا الَّذِينَ آمَنُوا خُذُوا حِذْرَكُمْ)

قال أبو جعفر:

(يعني بقوله جل ثناؤه : "يا أيها الذين آمنوا"، صدَّقوا الله ورسوله ="خذوا حذركم"، خذوا جُنَّتكم وأسلحتكم التي تتقون بها من عدوكم لغزوهم وحربهم).

وعن أبي هريرة - رضى الله عنه - عن النبي - صلى الله عليه وسلم - أنه قال: «لا يُلدَغُ المؤمنُ من جُحْرٍ واحد مرتين».

(رواه البخاري ومسلم).

من منطلق إيماننا الراسخ بضرورة تطوير قدرات الإخوة في الحركات الجهادية من نواحي الأمن التقني فإننا نقدم الجزء الأول من سلسلة كتب الحرب الإلكترونية والمتعلق بالأمن السيبراني وسبل الحماية.

رغم وجود التطبيقات العملية في الكتاب إلا أن الشروح النظرية التي قد تبدو لك أخي القارئ مملة أحيانا سوف تعطيك نظرة عامة وشاملة على كل ما سوف تتعلمه لاحقا.

فهدفنا من هذا الكتاب ليس التلقين والتطبيق وإنما الفهم العميق لآليات عمل أنظمة الحماية، وإننا ندرك أنك سوف تعود لهذه الدروس النظرية دوماً كلما استشكل عليك أمر ما.

ولا ننصح أن تقرأه دفعة واحدة، بل تلذذ به وتعمق على دفعات، اقرأ السطر مرة ومرتين، افهم الكلمات ولا تحفظها، تخيل البيانات وهي تنتقل من هنا لهناك وما يحدث خلف كواليس التطبيقات والبرامج، ثم قم ببحثك الخاص وتوسع أكثر، فالقراءة مفتاح العلم، والعلم مفتاح النجاة والنصر بإذن الله تعالى.

خذ وقتك اللازم، اشرب فنجان قهوة، اقرأ فقرة واحدة كل بضع ساعات، لا تنتقل للتي تليها ما لم تفهمها جيداً.

لسنا ولست على عجلة من أمرنا، فأعطي الأمر الوقت الذي يستحقه.

في الكتاب فإننا لا نقوم بالتوصية ببرامج معينة للحماية ولا شرح طرق استخدام برنامج محدد من بينها، إنما نعلمك مفهوم الأمن السيبراني وآلية الوصول لأفضل حماية ممكنة مع طريقة اختيار البرامج والآليات التي تناسبك، ونترك لك حرية البحث واختيار الأفضل بالنسبة لك.

إخوانكم في القسم التقني – فريق الحرب الإلكترونية

مجلس التعاون الإعلامي الإسلامي

تعريف الحرب الإلكترونية

إن مصطلح الحرب الإلكتروني مصطلح كبير وباب واسع للغاية، وغالباً ما يأخذ الجانب العسكري والميداني (خارج عالم الإنترنت) منه النصيب الأكبر.

وما الحرب السيبرانية إلا جزء ونوع من أنواع الحروب الإلكترونية، وإننا بإذن الله تعالى سوف نستمر بإصدار سلسلة الكتب هذه حتى نغطي مجال واسع من أنواع وطرق هذه الحرب التي لم تعد حرب المستقبل فقط بل هي حرب الحاضر والواقع كذلك.

ومن الأمثلة على الحرب الإلكترونية هي أنظمة الرادار العسكرية، الطائرات دون طيار، محطات الإنذار والمراقبة، معدات الرصد والمراقبة.

بينما من أشهر الأمثلة على الحرب السيبرانية هي عمليات اختراق المواقع الإلكترونية أو الشبكات والتحكم بها.



الحروب السيبرانية – حروب الحاضر والمستقبل

وتنقسم الحرب السيبرانية إلى ثلاثة أنواع رئيسية وهي:

أولا: الهجوم الإلكتروني عبر الإنترنت

ثانيا: دعم الحرب الإلكترونية باستخدام الإنترنت

ثالثا: الحماية الإلكترونية عبر الإنترنت

وفي هذا الجزء من سلسلة كتب الحرب الإلكترونية هذه سوف نسلط الضوء على النوع الثالث من الحرب السيبرانية وهو الحماية عبر الإنترنت، كيف تحمي نفسك في العالم الرقمي؟.

بينما سوف نقدم في أجزاء تالية النوع الأول من الحرب السيبرانية والذي سوف يرشدك إلى تنظيم هجمات إلكترونية لغايات إيقاف أو عرقلة عدونا، تكبيده الخسائر وإحداث حالات من الفوضى في صفوفه، فضلا عن البحث حول السبل المتاحة لتطوير هذه الهجمات لتشمل قطاعات مختلفة وصولا إلى الغاية الأسمى وهو الهجوم في سبيل السيطرة والتحكم على الهدف.

ثم في جزء خاص سوف نقدم النوع الثاني من الحرب السيبرانية، حيث سوف تتعلم السبل والوسائل التي تمكنك دعم الميدان من خلال الحرب السيبرانية، مثل حرب الشائعات والحرب النفسية والإختراق وسرقة المعلومات وغيرها من الوسائل.

وبالطبع لا يمكن المضي قدماً في النوع الأول والثاني مالم تكن ذو خبرة وعلم في كيفية حماية نفسك، وإلا فعندها ستكون عمليتك الأولى هي الأخيرة وهذا ما لا نقبله، فنحن نحذر دوماً من ممارسة الحرب السيبرانية دون علم ودراية تامة بوسائل الأمن السيبراني وكيفية حماية نفسك.

وأود التنويه إلى أن الحرب السيبرانية بحد ذاتها هي عالم كامل يكاد لا ينتهي من التفاصيل والوسائل، إلا أنني أيه القارئ الكريم سوف أتدرج به حسب المستطاع، واسأل الله التيسير لنا جميعا يا رب العالمين.

الأمن السيبراني

قبل بداية الحديث عن الوسائل والطرق المتبعة لحماية اتصالاتك عبر الإنترنت، لابد من تعريف "الإنترنت" فما هو وكيف يعمل؟

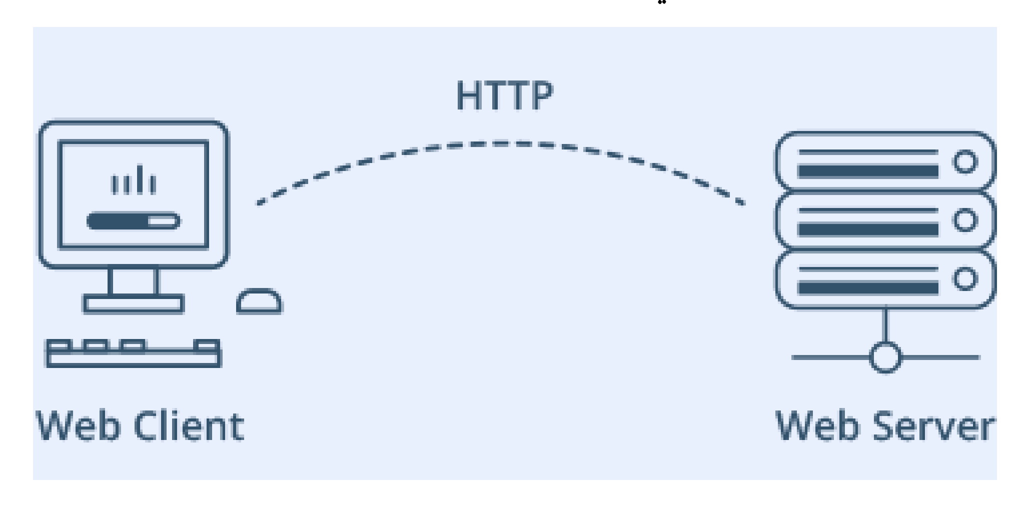
شبكة الإنترنت هي شبكة عالمية "لا مركزية". فلا يمكن بها الإجابة على سؤال مثل من يملك الإنترنت؟ في الحقيقة لا يوجد أحد حالياً يملك الإنترنت، هو بمثابة وقف عام لكل البشر.

تنتقل البيانات خلال هذه الشبكة بوسائل متعددة، للوصول إلى هدف واحد نهائي وغاية واحدة، الربط بين العميل والخادم ونقل البيانات بينهما باتجاهين.

العميل هو الشخص الذي يطلب البيانات، والخادم هو الجهة التي تقدم هذه البيانات.

على سبيل المثال: عند تصفح موقع جوجل فإن العميل في هذه الحالة هو أنت المتصفح، بينما الخادم هو شركة جوجل او سيرفرات شركة جوجل بصورة أكثر دقة.

وما بين العميل والخادم كلها وسائل وآليات مختلفة لبلوغ الهدف النهائي، وهو إجراء هذا الربط بين الطرفين، ونقل البيانات في كلا الاتجاهين.



العميل Web Client يقوم بطلب الخادم Web Server عبر بروتوكول التصفح HTTP

فمن الممكن أنك تتصفح شبكة الإنترنت من الهاتف الجوال، هنا يكون بينك وبين الخادم مجموعة من النقاط التي تنتقل خلالها البيانات وكذلك مجموعة من التطبيقات وأنظمة التشغيل، وهي التالية. (وقد يكون هناك المزيد فالأمر ليس ثابت دوماً)

- نظام التشغيل للهاتف -الأندرويد
- تطبيق متصفح الأنترنت -الكروم
- مزود خدمة الأنترنت -شبكة الهاتف
- مزود الأنترنت الرئيسي في البلد التي تتبع لها شركة الاتصالات

بينما في حالة تصفح الإنترنت عبر انترنت منزلي مثلاً، عندها عليك أن تضيف وسيلتين وهي الراوتر المنزلي، بالإضافة للسلك الموصل بينك وبين مزود الخدمة او البرج.

لذلك يمكن حصر انتقال هذه البيانات بطريقتين

- أولاً: سلكية
- ثانياً: لا سلكية

وقد يحدث ان تمر بياناتك عبر الحالتين، مثلا ان تنتقل بشكل لاسلكي من جوالك إلى مزود خدمة الإنترنت ثم يقوم هو بدوره بنقلها سلكياً عبر العالم.

الأمر لا ينتهي عند شركة الإنترنت ومزودها في البلد التي أنت بها، بل يتجاوز ذلك، لتوضيح الأمر دعنا نفترض أنك ترسل بريد إلكتروني من دولة عربية، يتم بدايةً تغليف البريد مع معلومات المرسل ومعلومات المستلم في حزمة واحده من قبل شركة البريد "الهوتميل"، الأمر يشبه تغليف شحنه لتوصيلها عند شركة توصيل البريد العادي.

ثم بعدها تنتقل هذه الحزمة من هاتفك او جهازك الكمبيوتر إلى الراوتر، ثم إلى أبراج الشركة، ثم إلى مزود خدمة الإنترنت الرئيسي في الدولة، والذي بدوره يرسلها عبر الأسلاك قاطعة دول مثل مصر، المغرب، عبر البحر إلى أوروبا ثم أمريكا. أو عبر البحر من تركيا إلى أوروبا ثم أمريكا، حسب الكيبل الرئيسي المغذي للإنترنت في المنطقة.

وهذا لأن شركة البريد الالكتروني -هوتميل- مقرها الرئيسي في أمريكا وسيرفراتها كذلك، فلا بد أن تصل حزمتك النهائي هناك.

هذه الآلية تنطبق على جميع أنواع التطبيقات، حتى تطبيقات المحادثة مثل التلجرام والواتس اب مع اختلاف دولة الشركة.

فمثلا إذا كانت الشركة للبريد الالكتروني روسية، فعندها سوف تمر حزمتك عبر نفس الطريق ولكن ستنتهي في سيرفرات الشركة الروسية بدلا من الأمريكية.

تخيل معي هذا المشهد في عقلك...

كتبت بريد إلكتروني عبر موقع او تطبيق "الهوتميل" أو "الجيميل"

قام الموقع أو التطبيق بتغليف الرسالة وعنوان المرسل وجميع بياناتك في طرد واحد ثم أرسله من هاتفك قاطعاً آلاف الأميال عبر العديد من نقاط توزيع الإنترنت وصولاً إلى جهته النهائية وهي خوادم أو سيرفرات شركة البريد الإلكتروني.

الخبر الصادم هو أن هناك عشرات الجهات في هذا العالم يمكنها التقاط هذا الطرد في اثناء رحلته هذه، والتي لا تستغرق أكثر من أجزاء من الثانية.

عشرات الجهات يمكنها التقاط حزمة بياناتك هذه في أثناء انتقالها من جهازك أنت العميل إلى الخادم!!

- ماذا يعني هذا؟ هل جميع حزم (طرود) بياناتي عرضة للسرقة؟

نعم، بالمعنى الحرفي هي عرضة للسرقة من كثير من الجهات.

- هل هذا يعني ان أمريكا يمكنها التجسس على حزم بيانات شركة روسية؟ أوالعكس؟

بالطبع يمكنها والسبب أنها ما زالت تستخدم شبكة إنترنت أمريكية ترتبط بقمر صناعي او كيبل إنترنت أمريكي.

- هل هذا يعني ان جميع اتصالات الروس ببعضهم تتجسس عليها أمريكا؟

لا بالطبع، لأن الروس وأي دولة في العالم وعلى نطاق حساس للغاية فهم لا يستخدمون قمر صناعي أمريكي ولا كيبلات أمريكية ولا شركات أمريكية، فتخرج الحزمة عبر إنترنت مملوك بالكامل لهم. وفي حالات أخرى فهم يقومون بتشفيرها بالطبع.

- أيهما أكثر أماناً، الإنترنت السلكي ام اللاسلكي؟

انتقال البيانات عبر وسط محمي وهو السلك الموصل بين العميل والخادم هو أكثر اماناً ، لأنه من السهل على الدول والجهات المختصة التجسس على بعضها البعض من خلال سرقة الحزم عبر انتقالها الفضائي بشكل لا سلكي.

الأمر يشبه إلى حد كبير جهاز "القبضة" اللاسلكية للتواصل بين الجنود، يمكن التجسس على اشارتها، والسبب هو انتقال هذه الإشارة عبر الهواء فيصبح لدى الجميع القدرة على الوصول إليها والتقاطها.

ولكن لا يمكن ابداً التجسس على مكالمة بين جنديين يتواصلان مع بعضهما عبر قبضة سلكية (جهاز الإرسال والإستقابل السلكي) حيث تنتقل بها الإشارة عبر وسط محمي بالكامل وهو السلك، لأنه في هذه الحالة يجب على الجهة الراغبة باختراق هذه المكالمة أن تضع شيء يقطع السلك نفسه لسرقة نسخة من البيانات أو إعادة توجيه الإشارة إلى جهة مختلفة.

- ماذا يحدث للحزمة التي خرجت من هاتفي بمجرد وصولها إلى سيرفرات الخادم؟

يتم فك الحزمة وقراءة بياناتها ومن ثم إعادة توجيه هذه البيانات إلى الشخص المتلقي.

وهو بدوره عند الدخول لبريده "في حال كانت الحزمة هي بريد إلكتروني" تنتقل حزمة مشابهة لها مرة أخرى من خوادم الشركة حتى تصل إلى جهازه.

- يبدو أن مهمة التجسس على الإنترنت سهلة للغاية!

ليس تماماً، على الرغم من أن معلوماتك وبيانات كلها عرضة للسرقة على طول الطريق بينك وبين الخادم! وعلى سبيل المثال لا الحصر فإنه من الممكن سرقة البيانات عبر إحدى أو جميع هذه النقاط

- الجوال نفسه إن كان مخترقاً
- تطبيق المتصفح الذي تستخدمه
- الراوتر إذا كان مزروع به برمجيات تجسس
- الأبراج ونقاط التوزيع إذا كان بها برمجيات تجسس
- مزود الإنترنت الرئيسي بالدولة
- جميع نقاط التقوية عبر سلك الإنترنت الرئيسي الذي يمر بالكثير من الدول حول العالم وصولاً إلى وجهة البيانات النهائية (وهذا الأخير يكون محمي بموجب اتفاقيات دولية)

نعم هذا صحيح فإنك معرض للسرقة في كثير من النقاط والأماكن، وليس فقط في الدولة التي أنت بها.

إلا أن الأمر ليس بالبساطة التي قد يبدو عليها...

فالخبر الجيد أن هذه الحزمة تنتقل بصورة مشفرة بالكامل، وهذا الأمر يعتمد على التطبيق الذي تستخدمه.

مثلا تطبيق التلجرام، عندما تكتب كلمة "مرحباً" وترسل إلى صديق.

يتم تغليف جميع بياناتك وتشفيرها بالكامل إلى حين وصولها إلى خوادم شركة التلجرام، وعليه حتى إن حاولت أي جهة على الطريق بينك وبين الخادم سرقة هذه الحزمة فهي لن تتمكن من معرفة ما يوجد داخلها ولن تستطيع فتحها.

وفي خوادم شركة التلجرام يتم فك الحزمة وإعادة توجيه الرسالة "مرحباً" إلى صديقك بعد تشفيرها من جديد.

- هل هذا يعني أن شركة التلجرام يمكنها التجسس على من تريد وقتما تريد؟

نعم بالضبط، وهنا يأتي دور مفهوم التشفير End to End

في هذا النظام من التشفير تضمن لك الشركة القائمة على التطبيق أن الحزمة لن يتم فك تشفيرها حتى في خوادم الشركة نفسها.

بل سوف يتم إعادة توجيه البيانات مباشرة إلى صديقك (المتلقي) وهي مشفرة بالكامل، حيث يتم فك التشفير في جهازه هو وتظهر له الرسالة "مرحباً".

وهذا هو أكثر وسائل التواصل اماناً -إن صدقت الشركة بالطبع ومثالنا هنا عن التلجرام-

- هل من الممكن أن تكذب شركات التطبيقات وتقول أنها تقدم خدمة تشفير كاملة وهي لا تفعل هذا؟

نعم قد تفعل وتكذب بخصوص هذه المزاعم، ولكن ليس في حالة تطبيقات ضخمة وعالمية مثل "الواتس اب" أو "التلجرام" فإن مئات ملايين البشر يستخدمونها، وهناك عشرات ومئات التطبيقات المنافسة التي تترصد غلطة واحدة لهم، وكذلك عشرات الجهات والفرق الإلكترونية الذين يعملون للتأكد من صدق الشركة فيما تدعيه.

ولهذا فإننا ننصح دوماً باستخدام التطبيقات العالمية المشهورة، اترك الأخرين يبحثون وفي حال وجود أي خلل أوشبهة في مزاعم التطبيق الأمنية عندها سوف نعلم ذلك من الآخرين.

- حسناً الوضع جيد جداً، إذا قمت بضامن أمن انتقال بياناتي عبر الإنترنت وتشفيرها فلا خطر بعدها..... صحيح؟

تقريباً هذا صحيح، لكن بالطبع كل ماتم ذكره أعلاه يكفل أمن البيانات بمجرد خروجها من جهازك حتى وصولها إلى جهاز المتلقي، بينما ما يحدث داخل جهازك فهذه مسؤوليتك أنت.

ففي حال كان الجهاز مخترق وتمكن شخص ما من سرقة بيانات الرسالة قبل تشفيرها من قبل البرنامج أوالتطبيق المستخدم فهو غير مسؤول عن هذا.

وهذه الحالات تحدث ونسميها الإختراق، أي تم اختراق الجهاز نفسه وعندها لن ينفع أي وسيلة تستخدمها لحماية بياناتك.

والسبب هو أن المخترق سوف يتجسس عليك أثناء كتابتك للبريد الإلكتروني، فعملية التشفير كلها في التطبيق تحدث بعد ضغطتك على زر الإرسال، وليس أثناء طباعتك للبريد، فالمخترق وبرمجياته الضارة سوف ترى جهازك بالضبط كما تراه أنت، وتسرق كل ما تفعله قبل أن يتم تشفيره.

وهنا فإننا ننصح مثلاً باستخدم برامج حماية الشاشة نفسها (سوف نتطرق لها بتفصيل أكثر لاحقاً) ، ولكن باختصار هذه التطبيقات سوف تمنعك من أخذ (سكرين شوت) أو صورة لقطة للشاشة وسوف تمنعك من تسجيل فيديو لشاشتك والكثير من الأمور الأخرى..

ماذا يعني هذا؟ هذا يعني أنه إن تمكن أحد من اختراق جوالك الشخصي فهو لن يرى إلا شاشة سوداء فقط، لأن هذه التطبيقات سوف تمنع التقاط أي صورة من الجهاز.

بالتأكيد ليست هذه وسيلة الحماية الكافية، حيث أن البرمجيات الضارة ليست بحاجة لرؤية شاشة جهازك كما تراه أنت، ولكنها واحدة من الوسائل وسوف نتطرق لها بالتفصيل لاحقاً.

من المقدمة أعلاه نصل إلى ضرورة تطبيق الآليات التالية للحماية...

أولاً: حماية الجهاز نفسه من الإختراق.

ثانياً: تأمين الجهاز في حالة تم اختراقه.

ثالثاً: استخدام تطبيقات تضمن التشفير End to End

رابعاً: إخفاء هويتك عبر الإنترنت بالكامل

لحماية الجهاز نستخدم تطبيقات برمجية خاصة مثل "مكافح الفيروسات"، "الجدار الناري" وتطبيقات حماية الشاشة نفسها.

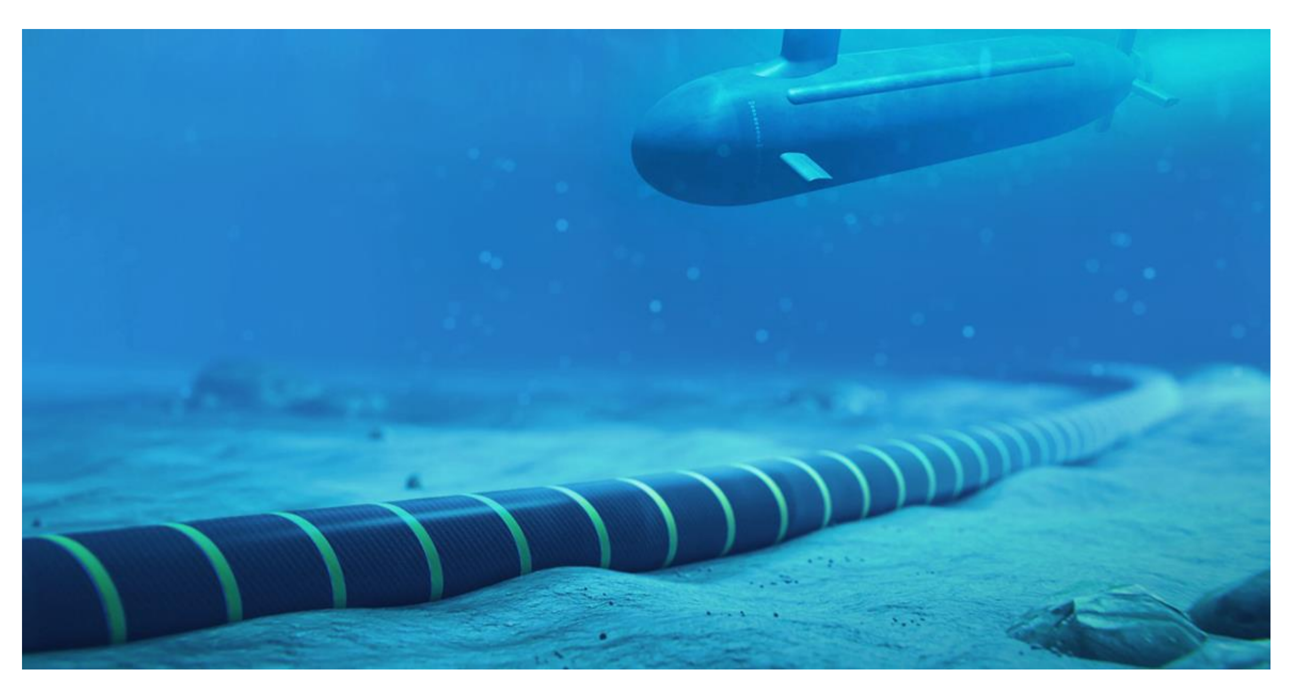
ولحماية الجهاز وتشفير الإتصال نستخدم الفي بي أن "Virtual private network VPN" والبرمجيات الخاصة بتشفير البيانات.

تنتهي مقدمة الأمن السيبراني وسوف نخوض في الفصول التالية بتفصيل أكثر حول وسائل الحماية المتبعة.

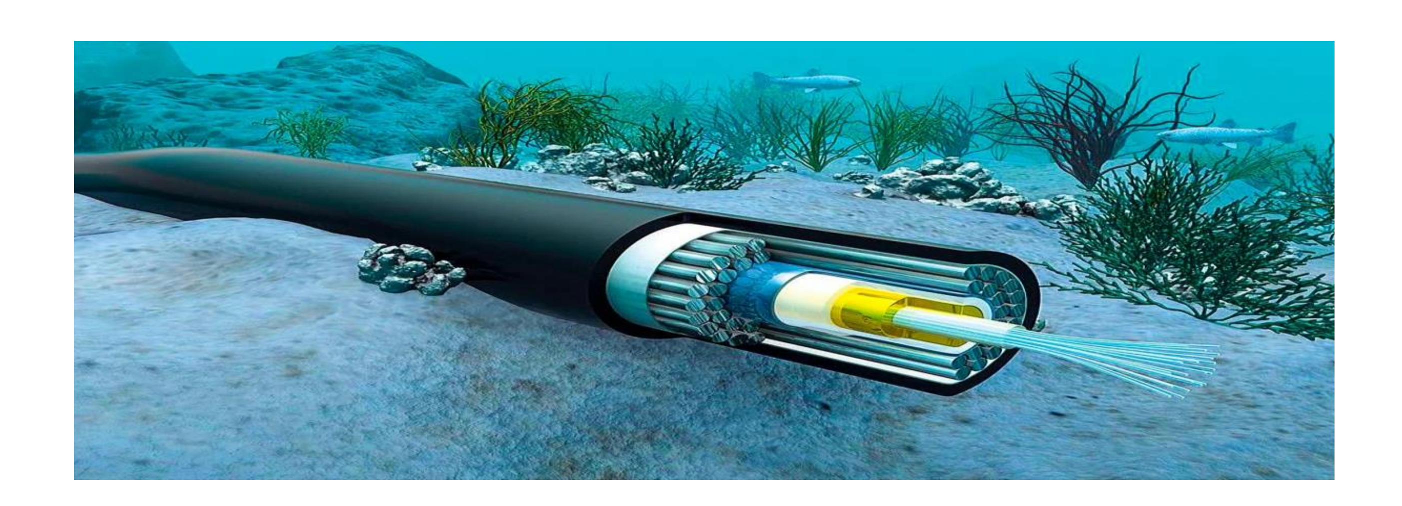
في نهاية هذا الفصل نود التنويه إلى أساسيات الأمنيات وهي عدم استخدام أي رقم حقيقي في التواصل أو في تفعيل حسابات مواقع الإنترنت وتطبيقات التواصل الاجتماعي.

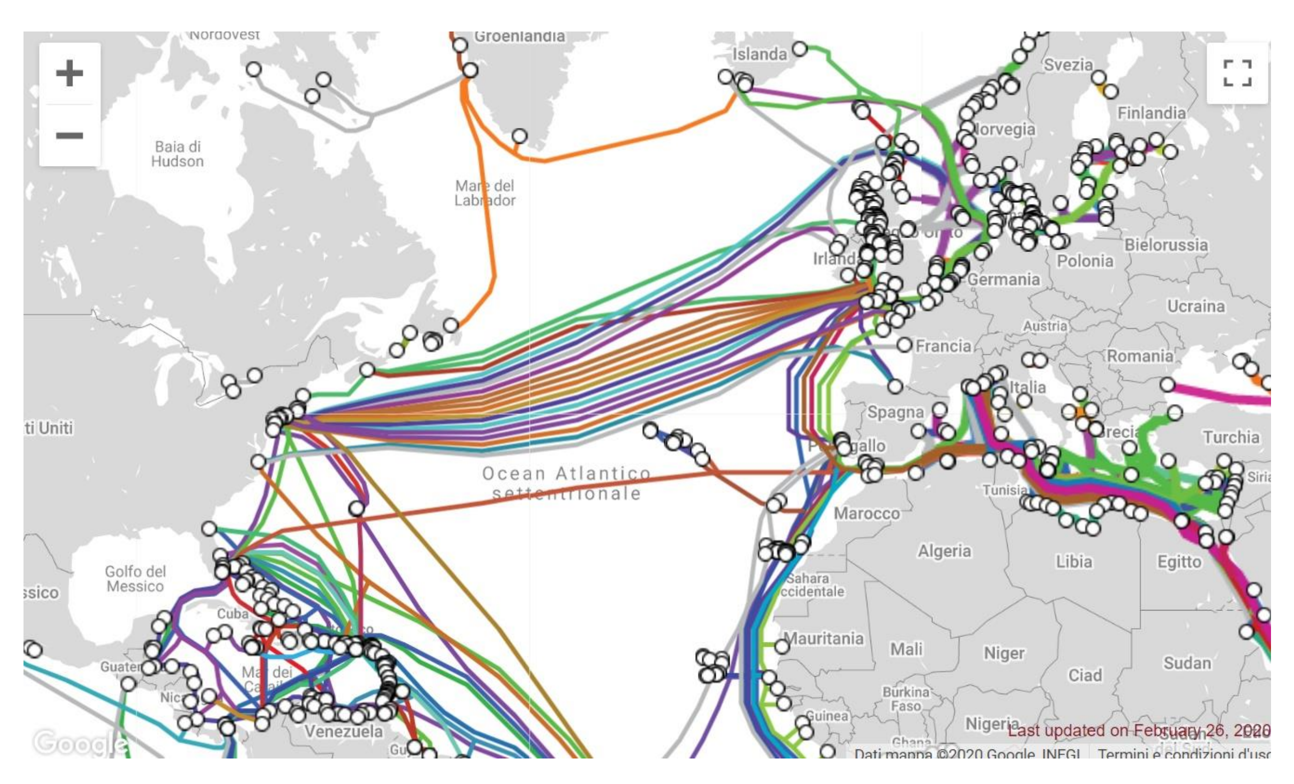
- من المهم دائما استخدام الأرقام الوهمية كما سوف يتم شرحه في الفصول التالية من هذا الكتاب.
- كذلك لا تستهين بخطورة كلمة المرور السهلة، اجعلها صعبة حسب التوصيات، حرف كبير وصغير ورقم ورمز.
- أيضاً لا تستخدم نفس كلمة المرور في أكثر من موقع، وهذا الخطأ يقع به الكثير من الإخوة للأسف، يستخدمون كلمة مرور واحدة في كل مكان.

لا تتردد بالتواصل معنا لتزويدنا بأفضل طرق الحماية التي إبتكرها أو استلهمتها من هذا الدرس وذلك عبر الطرق الرسمية المعتمدة.



تعتبر الكيبلات البحرية بمثابة العامود الفقري للإنترنت في العالم كله





يوجد حالياً أكثر من 430 كابلاً تحت الماء تعبر ما يقرب من 750.000 ميل (1.2 مليون كيلو متر) من قاع المحيط، يتبع الكثير منها لأمريكا حيث أنها تمتلك أكبر عدد من الكيبلات البحرية في العالم.

الفي بي أن (Virtual private network VPN)

- ما هو الفي بي أن؟ VPN

الشبكة الخاصة الإفتراضية (Virtual private network)، هي بروتوكول تشفير وحماية عبر الإنترنت، ببساطة وبدون تعقيد، الفي بي أن يعين نفسه وصي عليك وعلى هاتفك وعلى بياناتك، فلن يخرج كلمة من هاتفك ولن يدخل له كلمة، إلا عبر سيرفرات شركة الفي بي أن التي تستخدمها، والتي تكون منتشرة عبر العالم.

فعند استخدم تطبيق معين فإنه سوف يسطو على جهازك بالمعنى الحرفي، سيقوم بمنع دخول أي شيء وخروج أي شيء إلا من خلال المرور عبره أولاً، وعليه فهو سوف يحمي موقعك الجرافي "الآي بي IP Address" فكل البيانات تتم عبره وعبر الآي بي الخاص به.

فإذا كتبت "مرحباً" وأنت تستخدم الفي بي أن، فإن حزمة بياناتك لن تذهب إلى شركة "التلجرام" بل سوف تذهب إلى خوادم شركة الفي بي أن أولاً، ومن ثم هو من سوف يتولى إعادة توجيهها إلى التلجرام.

هذا يعني أن التلجرام نفسه لن يتمكن من معرفة عنوان الآي بي الحقيقي لك.

ليس فقط إخفاء الهوية، كذلك يعمل على تشفير إضافي لجميع الحزم الخاصة بك (ليس كل شركات الفي بي ان تقدم هذه الخدمة)، فإذا أرسلت رسالة على التلجرام، سوف يقوم بتشفير الحزمة المشفرة سلفاً من التلجرام، مما يعني ان شركة التلجرام نفسها لن يمكنها فك تشفير هذه الحزمة، حتى إن أرادت ذلك.

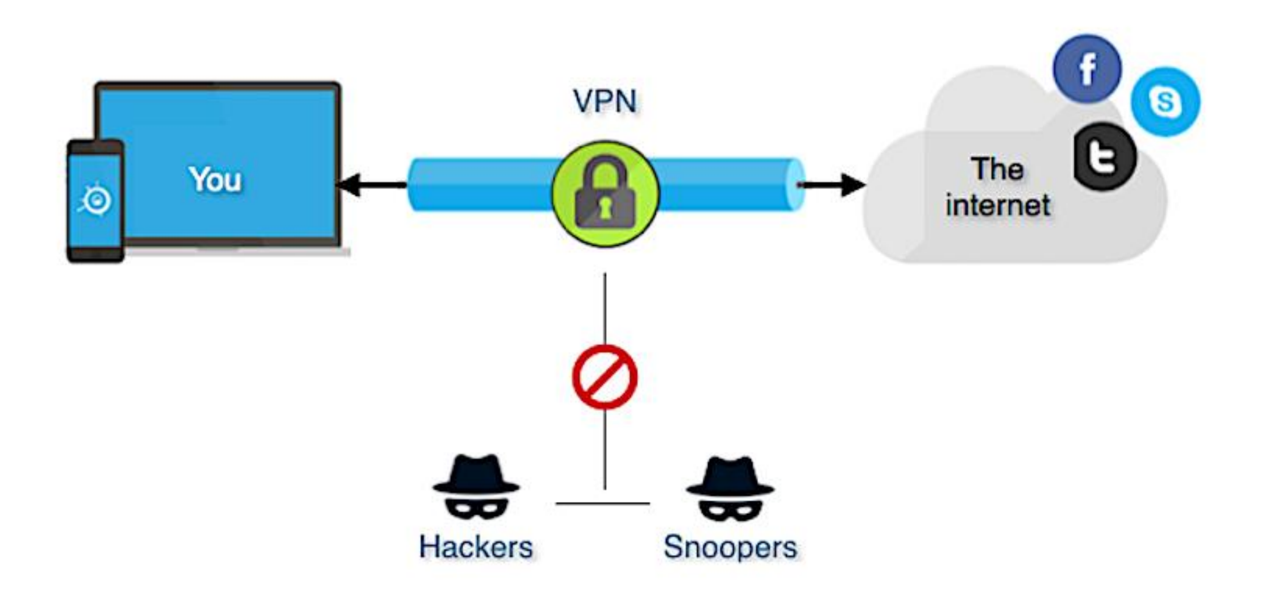
فالجهة الوحيدة المخول لها فك تشفير الحزمة هي شركة الفي بي أن.

وإذا شركة الفي بي أن فكت هذه الحزمة سوف تصطدم بتشفير التلجرام، والعكس.

وعليه إذا لم يكن هناك أي تنسيق بين شركة الفي بي أن والتلجرام على فك الحزمة فمن المستحيل أن تفكها جهة واحدة لوحدها.

فإذا قمت أنت بتركيب "في بي أن" صيني، واستخدمت تطبيق تراسل أمريكي، عندها لابد أن يكون هناك تفاهمات سرية بين الشركة الصينية والشركة الأمريكية ليتمكنوا من فك حزمتك. وذلك لأن كل جهة قامت بتشفير الرسالة بدورها، وعند فك التشفير سوف تصطدم بتشفير الشركة الأخرى.

وإذا قررت أن تعقد الأمور أكثر، وتدخل خادم روسي في الوسط بينهما، فعندها لابد أن يحدث تفاهم بين الثلاث جهات، ليتمكنوا من فك رسالتك المكتوب بها "مرحباً".



يقف ال VPN بينك وبين شبكة الإنترنت ويحمي خصوصيتك من المتطفلين ويقوم بتشفير بياناتك وإخفاء هويتك

الخلاصة المهمة هي التنوع

لابد بعد أن تكون قد فهمت آلية عمل الإنترنت والتجسس عليه، أن تحرص على أن تنتقل بياناتك عبر جهات متخاصمة وشركات يستحيل ان يكون بينها تفاهمات فيما يسمى "الحرب على الإرهاب".

- ولكن ماذا لو حدث تواصل وتفاهم بين الشركات؟ فالحرب على الإرهاب حرب عالمية وهذا موجود بالفعل والتنسيق قائم بين جميع دول الكفر العالمي!

حسناً في هذه الحالة عليك ان تقطع عليهم الطريق، من خلال استخدام في بي أن خاص.

وهذا موضوع ليس بالمعقد ولكن ليس بالسهل على أي أخ القيام به، لأنه يستلزم عمل سيرفرات وتركيب برمجيات تشفير داخلها، بحيث تنتقل الحزمة إلى الخادم الخاص بك وتشفيرها تشفير خاص بك، قبل أن ترسلها عبر العالم، والعكس.

ولكن هذا غير ضروري.

ورغم أنه قد يكون مطلوباً في مرحلة ما.... ولكن لا داعي لتعقيد الأمور على نفسك إلى هذا القدر، ما ذكرناه سابقاً كافي ووافي تماماً.

- كيف أختار أفضل تطبيقات الفي بي أن؟

قبل أي شيء أول ما عليك معرفته هو عدم إستخدام التطبيقات المجانية أبداً.

فكر للحظة، لماذا تقوم شركة بتصميم وبرمجة تطبيق يكلفها شهرياً مبالغ طائلة لتشغيله ثم تقدمه مجاناً لك؟ ماهو الثمن الذي سوف تدفعه بالمقابل؟

الثمن لن يكون بضع إعلانات يتوجب عليك مشاهدتها فقط، بل ستكون خصوصيتك هي الثمن الحقيقي الذي سوف تدفعه.

فالتطبيقات المجانية فضلاً عن انها تكون مصممة لغايات التشغيل فقط، ولا تقدم ميزات حماية أو شبكات إفتراضية قوية أو حتى تشفير حقيقي وجاد، فإنها تواجه تهم كبيرة بالتجسس على الخصوصية أو بيع المعلومات ومشاركتها مع جهات مختلفة.

وهذا لا يعني بالضرورة مشاركتها في ما تسمى الحرب على الإرهاب ...

بل إنها تبيع هذه المعلومات إلى شركات الدعاية الإعلانات مثلاً، ومراكز الدراسات والبحوث، وغيرها من الجهات العالمية الخاصة والعامة التي يهمها جمع البيانات، وبالطبع فالبيب من الإشارة يفهم، فمن يتاجر ببياناتك ويبيعها لشركات الدعاية والإعلان فإنه سوف يبيعها لكل من يدفع الثمن المناسب كذلك.

هل مازلت تذكر ما قلناه سابقاً عن استخدام التطبيقات والبرامج المشهورة عالمياً؟

نعم فهذه البرمجيات تكون تحت المجهر دوماً، عشرات المنافسين وفرق البحث والتقنيين يبحثون حول جدية ما تقدمة من حماية وأي شبهات لانتهاك الخصوصية.

لذلك فإن الأمر لن يكون مخفي عنهم إن فعلت شركة مثل هذا.

ولقد قمنا بالبحث حول توصيات المختصين لأغلب تطبيقات الفي بي أن المجانية كلها كانت توصي بعدم استخدامها لأسباب متعددة منها تهم بانتهاك الخصوصية ومنها ضعف في شبكاتها الإفتراضية وتسرب البيانات تقنياً ومنها عدم توفر تشفير قوي والعديد من الأسباب الأخرى.

بينما هناك الكثير من خيارات تطبيقات الفي بي أن الموصى بها عالمياً من قبل المختصين وللأسف فإن جميعها تطبيقات مدفوعة غير مجانية، الخبر الجيد هو ان أسعار الفي بي في متناول الجميع بمبلغ قد لا يتجاوز ال 5 دولار شهرياً.

التالي هي بعض أشهر انواع الفي بي أن المجانية، والغير موصى بها نهائياً

1- تطبيق SuperVPN

هذا واحد من أشهر التطبيقات، وهو تحديدا عليه توصيات سلبية بل تهم بالتجسس على المستخدمين

شاهد هذه الدراسة

https://www.safetydetectives.com/best-vpns/supervpn/#:~:text=Is%20SuperVPN%20safe%3F,visit%20and%20files%20you%20download

2- تطبيق Secure VPN

تقييمه 2 فهو مصنف غير آمن.

حسب هذا التحقيق والدراسة الأمنية التقنية التالية

https://vpnoverview.com/vpn-reviews/secure-vpn/

تقول الدراسة أن هذا التطبيق لا يحمي إتصالك بالإنترنت كما يتعهد، بل يتواجد به خلل تقني كبير يتسبب بتسرب معلومات الإتصال تقنياً، وهذا يعني أن عنوان الآي بي IP الخاص بك سوف يتسرب خلال إستخدامك لهذا التطبيق.

ورغم هذا فهناك خلل أكبر وغير تقني...

تقول الدراسة ان البرنامج أمريكي مسجل لشركة أمريكية رسمية وهذا يعني أن السلطات الأمريكية يمكنها سحب أي معلومات تريدها من خلال مذكرات الإستدعاء ، يعني من خلال المحكمة.

ولكن لحظة !!! إن الكثير من تطبيقات الفي بي أن أمريكية كذلك فهل هذا يعني ان بمقدورهم الحصول على أي معلومات يريدونها بمذكرة إستدعاء؟

بالطبع لا، وهنا يأتي دور التطبيق نفسه وميزة غاية في الأهمية، هل يقوم التطبيق أو برنامج الفي بي أن بحفظ البيانات من الأساس؟

كما ورد ذكره سابقاً فإن التطبيقات المجانية تقوم بهذا، والسبب هو أسباب تجارية فهذه البيانات، حركة مرورك عبر الإنترنت تعتبر مادة دسمة لتجارة الإعلانات والبحوث وغيرها، لذلك فهي تحتفظ بنسخة منها وهذا ما يفعله تحديداً هذا البرنامج.

وفي نفس الوقت التطبيق يطلب تسجيل دخول كامل، بريد إلكتروني ... الخ، وهذا فيه خطر مشاركة المعلومات مع السلطات الأمريكية.

3- تطبيق. Thunder VPN

للأسف يوجد عيب خطير في هذا التطبيق مشابه لما سبقه، وهو جمعه للبيانات

وعندما نقول جمعه لبيانات المستخدمين لا تعني بالضرورة أنه قدمها لجهات حكومية، ولكن اللبيب بالإشارة يفهم، من يجمع معلوماتك من أجل الأغراض التجارية فهو لن يتردد ببيعها كذلك لجهات حكومية.

الدراسة التالية تؤكد ذلك

https://www.top10vpn.com/reviews/thunder-vpn

هذه مشاكل التطبيقات المجانية، فعندما يقدم لك أحدهم شيء بالمجان عليك أن تعلم انك أنت السلعة.

عندما تقدم شركة تطبيق مجاني للفي بي ان ، لماذا؟

ماهي مكاسبها؟

بالطبع بياناتك وخصوصيتك واحده من أهم هذه المكاسب، حيث سوف تكون عرضة للبيع سواء لتجارة الإعلانات او لمراكز الدراسات او حتى لجهات حكومية.

- حسناً، سوف أبتعد تماماً عن التطبيقات المجانية، أخبرني كيف أختار التطبيق المدفوع وماهي هي معايير الإختيار التي علي اتباعها؟

أحد اهم الأمور التي تهم الباحثين في تحديد إن كان التطبيق آمن أم لا هو قيامة بحفظ سجلات للمستخدمين.

التطبيقات الآمنة لا تفعل هذا أبداً، فإذا دخلت موقع عبر الفي بي ان لن تحتفظ الشركة بأي نسخة بيانات من الآي بي الخاص بك أو البيانات المنقولة أو حركة مرورك عبر الإنترنت.

وطبعاً الأكثر أماناً هي تلك التطبيقات التي لا يتطلب التسجيل بها بريد إلكتروني ولا هاتف.

بالإضافة طبعاً لميزات التشفير التي يقدمها وباقي الخدمات التي سوف نذكر أهمها.

لاحظ ان موقع top10vpn يوصي بتطبيقات الفي بي أن في الرابط التالي كأفضل 10 تطبيقات، كلها مدفوعة وليس من بينها تطبيق مجاني واحد.

/https://www.top10vpn.com/best-vpn

وعلى سبيل المثال لا الحصر، سوف نقوم بشرح كيفية إختيار التطبيق الآمن بتجربة عملية على واحد من أشهر تطبيقات الفي بي أن العالمية وأكثرها تقييماً، برنامج البروتون Proton.

تطبيق بروتون تقييمه 8.8 من 10 وهذا تقييم ممتاز.

شاهد الدراسة الأمنية التالية

/https://www.security.org/vpn/protonvpn/review

الميزات التالية هي ميزات مطلوبة في أي برنامج في بي أن ويقدمها برنامج البروتون

1- لايقوم بتحزين أي بيانات نهائياً طوال فترة استخدامك له No Data Logging
2- لديه خيار "الكيل سويش Kill switch" وسوف يتم شرحه لاحقاً
3- تقسيم البيانات عبر الأنفاق وهذه ميزة أمان إضافية Split Tunneling
4- أي بي IP مشترك، وهذه ميزة أمان إضافية Shared IP address with other users
5- تشفير البيانات بالكامل أثناء إنتقالها من جهازك والعكس Network traffic encryption
6- سريع للغاية ولا يتسبب ببطىء في استخدام الإنترنت
7- يدعم شبكة التورينت Torrenting

التالي هي الملاحظات السلبية التي سُجلت على برنامج البروتون حسب الدراسة أعلاه

1- يتطلب تسجيل الدخول ببريد إلكتروني (للأسف أغلب البرامج تفعل ذلك وهي ميزة غير مرغوب بها)
2- السعر مرتفع للغاية مقارنة مع البرامج المنافسة
3- الدعم الفني بطيء

- ما هي خاصية الكيل سويش (Kill Switch) في برامج الفي بي أن، وكيف أقوم بتفعيلها؟

خاصية Kill Switch أو زر القتل توجد بتطبيقات الفي بي أن المميزة وهذا الخيار عند تفعيله فإنه سوف يعمل على قطع الإنترنت بشكل كامل من جهازك إلا من خلال الفي بي أن، فهو لن يجعل الإنترنت يعمل دون عمل الفي بي ان أولاً، فلا يوجد مجال للخطأ.

لكن في حالة عدم تشغيل ال Kill Switch

وعلى فرض أنه قد حدث خطأ في الفي بي أن عندها فقد تم فضح اتصالك لان الإنترنت سوف يستمر بالعمل بشكل طبيعي بدون الفي بي أن الى ان يعود للعمل ويحميك من جديد.

وخلال هذه الثواني التي يحدث بها هذا الخطأ سوف تكون مكشوف في العراء، بلا أي ميزات من الحماية التي يقدمها لك الفي بي أن ودون أن تعي أو تدرك هذا.

لذلك فإننا نوصي بشده أن تقوم بتفعل خيار Kill Switch داخل الفي بي أن، وهذا من إعدادات البرنامج

بالإضافة إلى ذلك فإننا نوصي بتفعيل الخيار التالي أو ما يشابهه دوماً

launch on start up التشغيل التلقاء عند تشغيل الجهاز

وهذا الخيار مع الكيل سويش سوف يعمل على قطع الإنترنت عن جهازك مباشرة عند الإنتقال من وضع الإطفاء إلى وضع التشغيل إلى حين إنتهاء الفي بي أن من التشغيل الكامل ثم السماح بمرور البيانات من خلاله فقط.

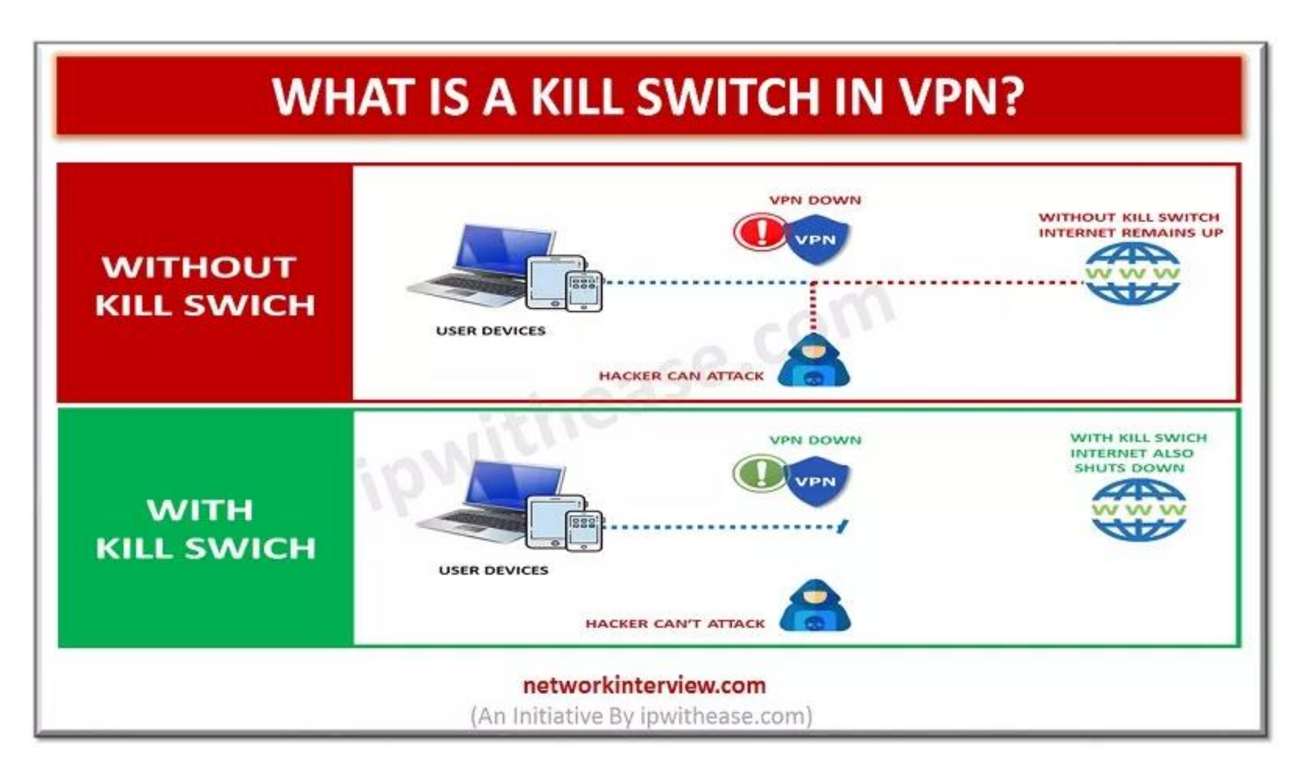
بينما في حالة عدم تفعيل هذه الخيارات فإن شبكة الإنترنت سوف تمر من وإلى جهازك قبل إنتهاء إقلاع الفي بي أن لثانية واحدة ربما، لكن هذه الثانية قد تكون الفارق بين الحياة والموت.

فالكثير من التطبيقات تعمل في خلفية الجهاز، مثل التلجرام والواتس أب، وقد تلتقط الأي بي الحقيقي الخاص بك خلال جزء من الثانية.

عندما يكون الفي بي أن في وضع التفعيل سوف يظهر في الهاتف على شكل مفتاح بجانب الساعة غالباً او بالطرف الأخر من الشريط العلوي.

للتأكد من انه يعمل ببساطة قم بفحص الأي بي الخاص بك عبر أي موقع لفحص الأي بي مثل هذا https://www.iplocation.net/

إن تم عرض أي بي IP يشير إلى دولة الفي بي أن التي اخترتها فهذا يعني انه يعمل، بينما إن ظهر أي بي يشير إلى بلدك الأصلي فعندها فإن التطبيق يواجه خلل في العمل.



في حالة تشغيل Kill Switch فسوف تبقى محمي حتى إن تم قطع خدمة ال VPN وذلك من خلال قطع إتصالك مع شبكة الأنترنت بالكامل

وهنا لا بد من الإشارة إلى ما يمكن تسميته بالنقطة الصفرية.

فماذا إن اشتريت هاتف لأول مرة، لابد حينها من الدخول للإنترنت لتحميل تطبيق الفي بي أن نفسه أول مرة، فإن دخلت على متجر جوجل فسوف يعرفون رقم الأي بي الخاص بك عن طريق البريد الإلكتروني الذي قمت بعمله لتتمكن من دخول متجر التطبيقات وبالتالي معرفة معلومات جهازك وبشكل خاص رقم IMEI الفريد الخاص بالهاتف الجوال.

حسناً سوف تقوم بعدها لا محالة بتركيب الفي بي أن، وعمل باقي إجراءات الحماية الخاصة والتي تعلمتها وسوف تتعلمها في هذه الدروس، وبعدها ستحذف البريد الإلكتروني وتغيره ثم تبدأ في إستخدام الجهاز في عملك الجهادي.

هل أنت في أمان تام عندها؟

كلا، فقد وقعت سلفاً في الخطأ الصفري وتركت خلفك كسرة خبز قد تدل عليك يوماً ما.

السبب هو أن رقم IMEI الفريد لجهازك مسجل حالياً في سيرفرات شركة جووجل ومرتبط به بريد الإلكتروني ذلك الذي توقفت عن استخدامه ولكن يرتبط به أيضاً عنوان الأي بي الخاص بك والحقيقي الذي قمت بإنشاء البريد من خلاله واستخدام متجر التطبيقات في تحميل الفي بي أن.

وبعد وقت طويل قد تنسى أنت هذا، ولكن جووجل لن تنسى، وفي حال سقط IMEI جهازك الخاص بيد أجهزة المخابرات بأي طريقة كانت، مثل أن تقوم بتحميل تطبيق غير موثوق أو تقع بخطأ تقني غير مقصود أو حتى من خلال التطبيقات الموثوقه إن كنت مطلوب دولياً على سبيل المثال، فعندها قد يتم الاستعانة بشركة جووجل للبحث عن IMEI جهازك وسوف يصلون إلى كسرة الخبز القديمة التي تركتها خلفك، وإلى الأي بي الذي استخدمته في ذلك الوقت.

ماهو الحل إذاً في هذه الحالة؟

جميع تطبيقات الفي بي ان لديها موقع الكتروني يمكنك تحميل نسخة التطبيق منها، لا تقوم ابداً بتحميل نسخة تطبيق من غير الموقع الرسمي للشركة فقط.

حيث تقوم بتحميلها على شكل ملف APK دون الحاجة لدخول متجر جوجل.

لذلك فإننا ننصحك قبل أن تبدأ إستخدام متجر التطبيقات أن تقوم اولاً بتحميل تطبيق في بي أن موثوق ثم تبدأ عمل باقي إجراءات الحماية.

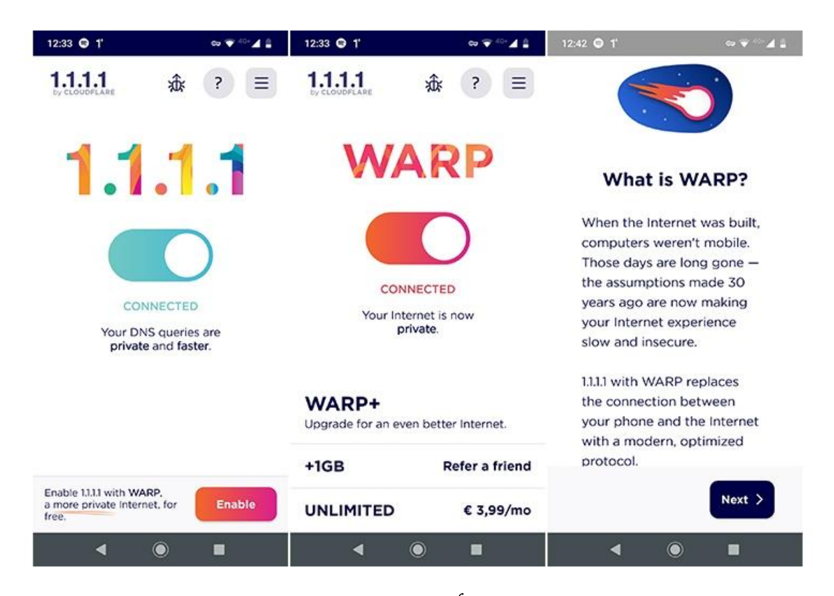
- هل يمكن تشغيل تطبيق في بي أن مع تطبيق تشفير إضافي أثناء العمل؟

نعم بالطبع، وهذا نوصي به بشده.

على سبيل المثال برنامج 1.1.1.1 أو ما يسمى Cloudflare WARP هو أحد خدمات شركة Cloudflare ذائعة الصيت في مجال التشفير والحماية عبر الإنترنت.

ورغم ما يشاع عنه أنه نوع من أنواع الفي بي أن، إلا ان هذا غير صحيح بتاتاً، فهذه الخدمة ليست بديلاً ابداً عن الفي بي أن، وإنما هي خدمة ثورية في مجال التشفير حيث سوف تنتقل جميع بيانات من جهازك وإلى جهازك مشفرة بالكامل عبر Cloudflare WARP.

إذاً لا يمكننا إعتباره بديلاً عن الـ VPN أبداً، ولكن هذه الخدمة هي خدمة ثورية في مجال التشفير والسرعة، فاذا كنت تريد المزيد من الحماية، استخدمه بالطبع مع في بي ان دون جدال، فسوف يقدم لك استخدام خدمة تشفير إضافية غير تشفير الفي بي أن طبقة حماية إضافية مختصة بالتشفير.

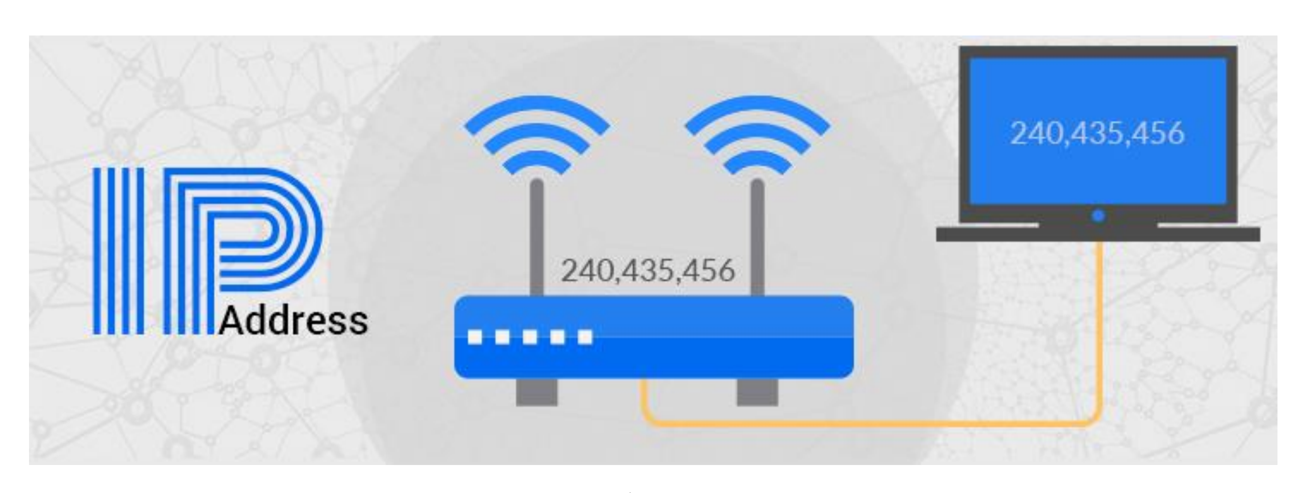


Cloudflare WARP تعمل على تأمين وتشفير جميع تواصلاتك عبر الإنترنت

بروتوكل عناوين الإنترنت IP address

- تحدثت كثيراً عن الأي بي (IP Address) فما هو وكيف يعمل؟

عنوان الأي بي IP Address ويعرف بالإنجليزية بـ Internet Protocol هو بروتوكول الإنترنت للعناوين، حيث تتعرف من خلاله شبكة الإنترنت على عناوين الأجهزة المرتبطة بها، ويمكنك إعتباره بالضبط كأنه عنوان منزلك التفصيلي بالشارع والرقم والبناية في حين أن الإنترنت هو صندوق بريد المراسلات اليدوية التقليدية، فليتمكن أحدهم من إرسال رسالة بريدية إليك فهو يحتاج إلى عنوان منزلك التفصيلي، وحسب نفس هذا المفهوم فإن عنوان الأي بي الخاص بك هو عنوانك التفصيلي الذي سوف يدل باقي أجهزة شبكة الإنترنت إلى جهازك.



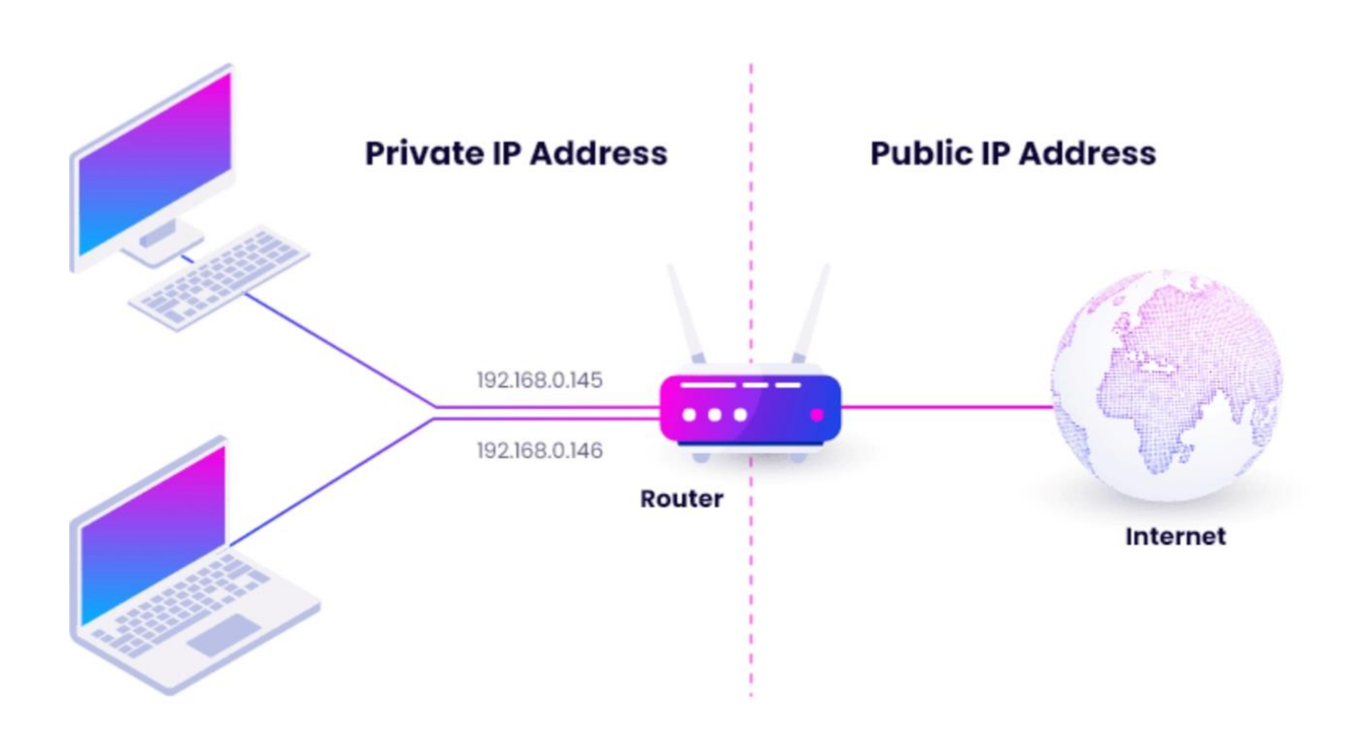
بروتوكل عناوين الإنترنت هو الطريقة التي تتعرف بها الأجهزة على بعضها البعض في الشبكة المعلوماتيه

وحسب المفهوم التقليدي فإن كل جهاز يرتبط بالإنترنت يمتلك أي بي خاص به باللحظة الزمنية نفسها، إلا ان هذا المفهوم غير دقيق تماماً.

فعلى سبيل المثال عندما يرتبط عدد من الأجهزة مع راوتر واحد فإن الأي بي لجميع الأجهزة سوف يكون هو نفسه وهو عنوان الأي بي الخاص بالراوتر، بينما سوف يقوم الراوتر بتمييز الأجهزة عن بعضها البعض من خلال أي بي داخلي أو محلي يسمى Local IP Address.

فعندما تقوم بالإرتباط مع الإنترنت عبر جهاز راوتر منزلي مثلا فإن عنوان ال IP العام الخاص بك سوف يكون هو عنوان ال IP لجميع الأجهزة الأخرى المرتبطة مع نفس الراوتر المنزلي، بينما سوف يقوم الراوتر بدوره بفرز هذه الأجهزة حسب أي بي محلي أو داخلي وهو الـ Local IP Address.

إذاً فبمجرد دخولك إلى الإنترنت فإنك تستخدم عنوانين للآي بي، العنوان العام الذي سوف يدل الشبكة على آخر نقطة توزيع إنترنت أنت مرتبط بها، ثم العنوان الخاص والذي سوف يدخل نقطة التوزيع هذه على جهازك بالتحديد من بين الكثير من الأجهزة الأخرى المرتبطة معها.



عنوان الآي بي العالمي (Public IP) يدل شبكة الإنترنت إلى الراوتر (Router)، بينما عنوان الآي بي المحلي (Private IP) يخبر الراوتر إلى أي جهاز عليه تسليم هذه البيانات ومن أي جهاز استلمها

- هل كل ما يحتاجه مخترق الأجهزة عبر الآي بي هو معرفة العنوان فقط؟

بالطبع لا، بالتأكيد سمعت عن خطورة عنوان الآي بي، وهو خطير بالفعل إن وقع بيد جهة ما يمكنها تحديد عنوانك التفصيلي واسمك ربما كذلك.

ولكن في حالات الإختراق فمعرفة عنوان الآي بي العام والخاص غير كافي ابداً.

فهذا العنوان معروف ويمكن للجميع معرفته بطرق عديدة كما أن كل موقع إلكتروني تدخله يمكنه معرفته كذلك مالم يمكن يستخدم تقنيات خاصة بحماية الزوار وإخفاء هوياتهم مثل التي تقدمها بعض الخدمات السحابية للمواقع الإلكترونية.

ومعرفة هذا العنوان لا تعني بالضرورة اختراق الجهاز، حيث أن المخترق يحتاج لأمر أخر غاية في الأهمية وهو المنفذ أو Port الذي سوف يخترق الجهاز من خلاله أو ما يطلع عليه مجازاً بالباب الخلفي.

وفي حين أن الآي بي العام و المحلي سوف يقود البيانات إلى جهازك مباشرة، إلا أن هذه المعلومات بمجرد وصولها داخل جهازك فهي ما زالت إلى الأرشاد! أين تذهب تحديداً؟

لنفرض أنك طلبت موقع جووجل عبر المتصفح، في هذه الحالة سوف يصل طلبك إلى شركة جووجل وبدورها سوف تعيد لك صفحة جووجل الرئيسية.

ولكن كيف سوف تعلم ان الذي طلبه هو فلان أي كيف سوف تستدل عليك؟ هذا يكون من خلال الآي بي االعام والمحلي ، فهي لن تعيد المطلوب لك تحديداً بل سوف ترسله إلى مزود الإنترنت الخاص بك ، وشركة الإتصالات سوف تستلم الطرد أو الحزمة وعليها عنوان المستلم، وهو الآي بي الخاص بك وسوف تسمح لها بالمرور إلى الراوتر الذي بدوره سوف يمررها إلى الجهاز عبر الآي بي المحلي.

ولكن بعد هذا أين سوف تذهب الحزمة في جهازك تحديداً

هنا يأتي دور المنفذ أو البورت Port.

البورت 80 على سبيل المثال هو بورت محجوز لبروتوكل التصفح HTTP

فعندما يرى الجهاز أن هذه الحزمة أو الطرد مطلوب تسليمها إلى بورت 80 فهو تلقائياً سوف يوجهها إلى المتصفح.

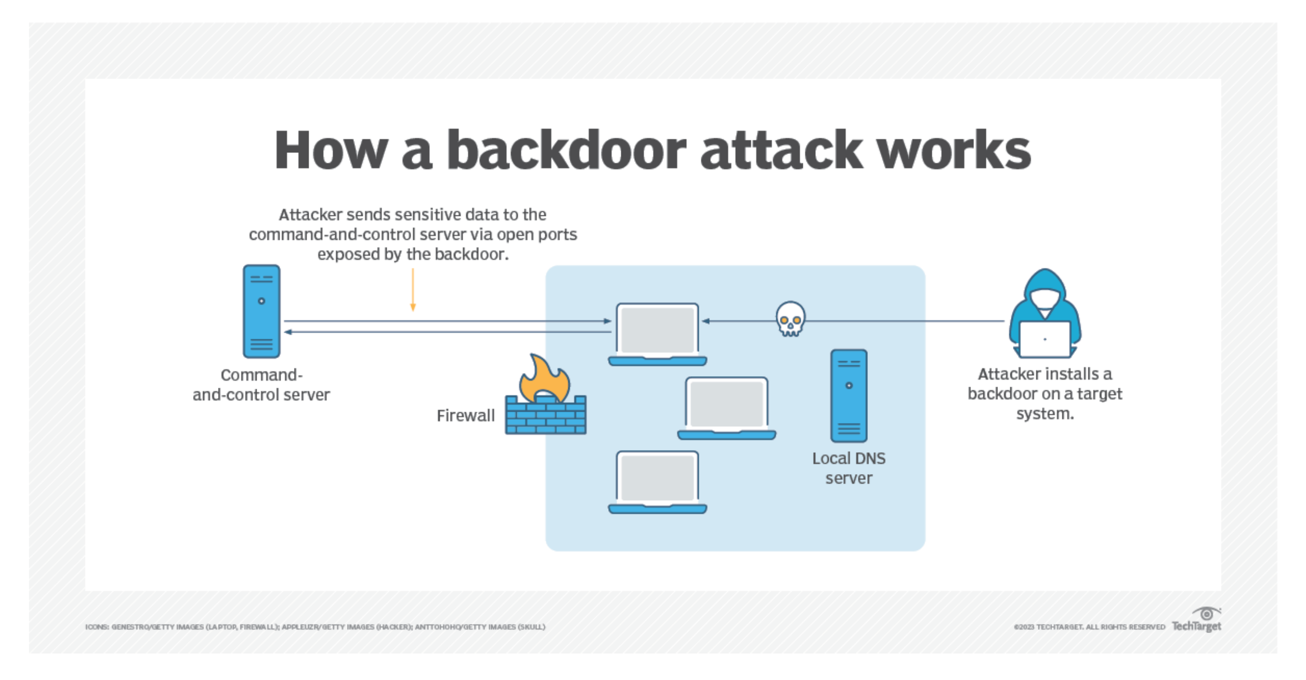
وعليه مثلا إذا تم إختراقك فإن المخترق سوف يفتح بورت خاص به مثلا 8022 وعبر هذا البورت سوف يتم ارسال البيانات إليه وكذلك استقبال أي أوامر منه، وهذا دون أن تعلم أو تشعر بذلك، وهذا ما نسميه بالباب الخلفي Back Door.

بعض البورتات تكون محجوزه سلفاً من نظام التشغيل مثل بورت 80 ولكن الجهاز يمكنه فتح ما يقارب 65000 بورت في اللحظة الواحدة.

وأقرب مثال على خطورة المنافذ هو المنفذ 3389 الشهير.

هذا المنفذ محجوز للإتصال البعيد مع الجهاز، ربما تعرف هذا الأمر عندما تقوم طوعاً بالسماح لشخص آخر أن يدخل جهاز كمبيوترك عن بعد ويستخدمه.

لذلك فإن أغلب أنواع الجدار الناري سوف تحظر هذا المنفذ تلقائياً لأنه خطير للغاية يمكن من خلاله دخول جهازك عن بعد، ولكن هذا لايعني ان برمجيات التجسس لا يمكنها فتح بورت أخر لنفس الغاية.



يقوم مخترق الأجهزة بتجاوز جميع أنظمة الحماية ويتواصل مع البرمجيات الخبيثة من خلال باب خلفي تقوم بفتحها له

وبالعودة إلى تطبيقات الفي بي أن وبرامج الحماية، فإن بعض أنواعها تسمح لك بإغلاق جميع المنافذ في الجهاز، ما عدا تلك الأساسية أو التي تستخدمها او تحددها انت، وعندها حتى إن كان هناك منفذ خلفي مجهول يستخدمة مخترق ما فإنه لن يعود قادر على إستخدامه.

فلن تتمكن هذه البرمجية من نقل او استقبال شيء ، وكأنك تسجنها داخل جهازك.

طبعا مالم تكن هذه البرمجيات تستخدم بورت أساسي في النظام، مثلا سمعت من قبل بالتأكيد عن الطابعات واختراق الأجهزة من خلال الطابعة ...

هذا لأن بعض برمجيات التجسس تستخدم بورت الطابعة الإفتراضي لنقل البيانات من خلالها.

تطبيقات الفي بي أن هذه سوف تحجب حتى بورت الطابعة مالم تكون تستخدمها وصرحت بفتح هذا البورت لوقت معين إلى حين انتهاء الطباعة.

إذا أردت حماية نفسك أكثر عليك دوماً تغيير البروتات الإفتراضية

مثلا البورت 3389 للاتصال عن بعد

ففي حالة كنت تستخدم هذا البورت وتحتاجه عندها الافضل تغييره الى رقم أخر مثلا 9911، ففي هذه الحالة لن يعلم المخترق ماهو بورت الاتصال عن بعد لديك.

ابحث عن طريقة تغيير البورتات في الجهاز.

ننصح باستخدام برامج الفي بي أن التي تقدم خدمات تغيير أرقام البورتات الإفتراضية والتي تسمح لك مراجعة وإغلاق جميع البورتات المشبوهة.

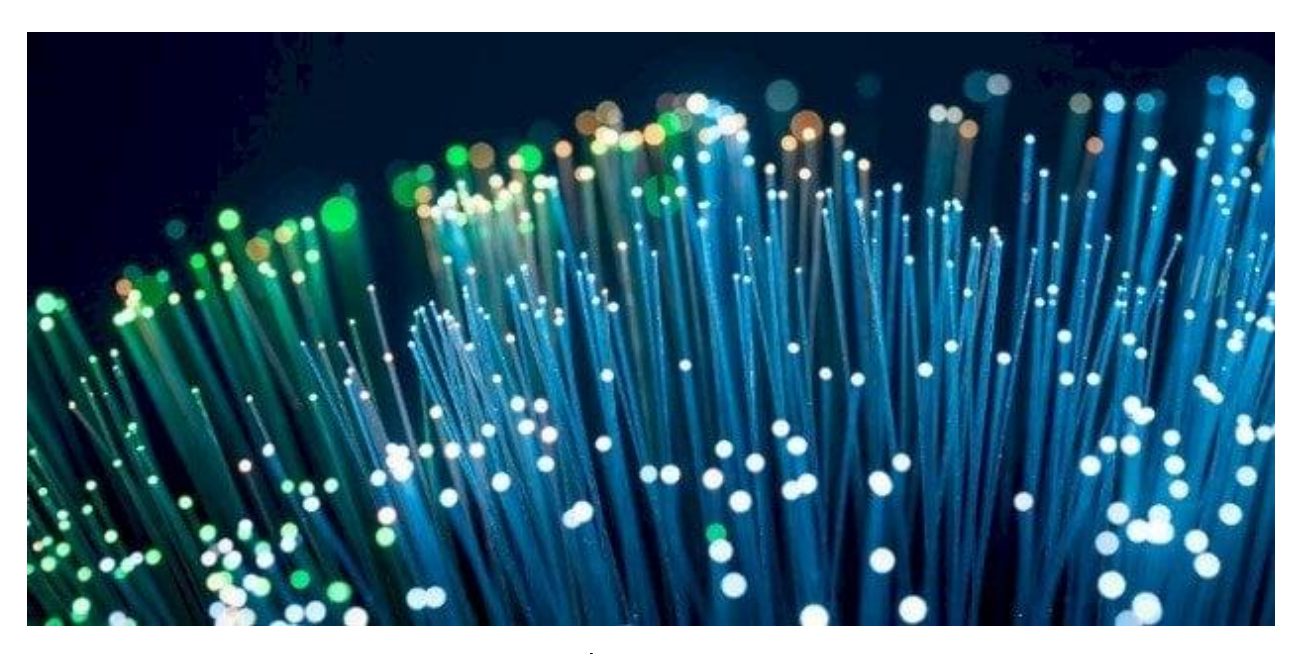
كواليس أبراج الإنترنت ومثال إدلب

في بداية هذه الدروس بينا أن الإتصال بشبكة الإنترنت يتم بواسطة طريقتين هما الإتصالات السلكية والإتصالات اللاسلكية.

بالطبع الإتصال السلكي أسرع كثيراً جدا من الإتصال اللاسلكي والسبب هو إنتقال البيانات بسرعات عالية عبر وسط محمي دون وجود أي مؤثرات جانبيه، هذه السرعة تساوي سرعة الضوء أي بسرعة الفوتونات . فكل إشارة سواء تلفاز أو انترنت أو راديو .. الخ هي في أصلها فوتونات وتتحرك بسرعة الفوتونات.

والفوتونات جسيمات غاية في الصغر تنتمي لعوالم ما دون الذرة، ولا تمكن رؤيتها ولا تتحقق رؤية شيء دونها، كونها المسؤولة عن نقل الضوء لشبكة العين التي تحوله إلى نبضات كهربائية.

قديما كانت الوظيفة الأساسية للفوتونات هي تحقيق عملية الإبصار من خلال نقل الضوء للعين، لكن هذه الجسيمات باتت تقوم بأدوار أساسية في كل مناحي الحياة، فقد مكنت العلماء من توظيف الأمواج الكهرومغناطيسية وأمواج البث الإذاعي والتلفزيوني، وصناعة أجهزة التحكم عن بعد وموجات الإتصالات التي تلتقطها الهواتف النقالة وأجهزة هبوط الطائرات وإقلاعها والشبكات اللاسلكية.



تنتقل الفوتونات عبر الألياف الضوئية أو البصرية بسرعة الضوء

حسناً بعيداً عن السرعة في نهاية الأمر سوف تنطلق هذه الفوتونات حاملة بياناتك عبر الأسلاك إلى وجهتها، إذا ضمنا بطريقة ما عدم وجود أي اختراق للسلك مثل تركيب أجهزة تجسس وسرقة البيانات عليه فنحن في أمان مطلق.

ولكن الأمر لا يحتاج اجهزة تجسس إن تم نقل هذه البيانات عبر الفضاء الكوني، او في الهواء مثلاً بما أننا نتحدث عن كوكب الأرض.

فهذه الفوتونات سوف تطير عبر الفضاء أي أن أي شخص يمكنه التجسس عليها، وذلك لأنه لايوجد عنوان ثابت تعرف أين تذهب له هذه الفوتونات.

مثلا في القبضة أو جهاز الإتصال اللاسلكي

عندما تتحدث به وتقول "مرحباً"

هذه الاشارة سوف تنطلق في الفضاء وكل جهاز إتصال لاسلكي متواجد في محيط قوة الإشارة أي في محيط مثلا 10 كيلو متر سوف يستطيع التقاط الإشارة وسماعها إن عرف درجة الموجة التي تم بثها عليه.

الموجة هي مثلا موجة الراديو إف إم، عدل الموجة وسوف تسمع إذاعة مختلفة عن الأولى وتكون هذه الموجة محجوزه لإذاعة معينة، وكل دولة تبيع هذه الموجات للإذاعات، ولهذا إذا كنت في منطقة حدودية ومعتاد على ان الموجة رقم 99 مخصصة لإذاعة القرآن الكريم فإنك قد تتفاجىء أن هذه الموجة لم تعد تلتقط إذاعة القرآن الكريم بل باتت تلتقط إذاعة للدولة الأخرى على الطرف الأخر من الحدود، هذا لأن تلك الدولة تكون قد باعات الموجة هذه على أرضها لإذاعة مختلفة، ولأن بث تلك الإذاعة أقوى من إذاعة القرآن فموجتها سوف تطغى ، وفي كثير من الأحيان سوف ترى صراع بين الإذاعتين، هذه تبث تارة ثم الأخرى وهكذا. يعني يحدث تداخل موجات.

بالعودة إلى أبراج الإنترنت...

بالتأكيد الإتصال السلكي هو الأكثر اماناً ولكن من هذا الذي يستطيع مد الأسلاك في كل مكان يصله الإنترنت؟ هذا الحل لن يكون عملياً بالتأكيد، لذلك فإن بث البيانات بطريقة لا سلكية هو الحل الأنجع والأسرع والأفضل، وهنا يأتي دور أبراج الإنترنت أو أبراج الإتصالات.

عندما ترسل بياناتك إلى برج هذا يعني انك أرسلتها بطريقة لاسلكية وهو سوف يعيد بثها بطريقة لا سلكية.

الحقيقة أبراج الإنترنت هي مجرد أبراج تقوية لا أكثر ولا أقل (بالمفهوم البسيط). وضيفتها التقاط الإشارة ثم إعادة بثها.



تعمل أبراج الإنترنت على إستقبال البيانات وإعادة بثها وصولاً إلى المزود الرئيسي

فإن كانت الإشارة الخارجه من جهازك تصل إلى 10 كيلو متر كحد اقصى فهذا يعني أنك بحاجة إلى برج بعد 10 كيلو يقوم بتقوية البث وايصال هذه الإشارة إلى برج أخر يبعد 100 كيلو متر وهكذا حتى تصل الإشارة إلى مركز الإنترنت الرئيسي في الدولة الذي قد يبعد عنك 2000 كيلو متر.

ولكن هذا كله بسرعة الضوء، أي سرعة الفوتونات، والتي يمكنها قطع 300 ألف كيلو متر في الثانية الواحدة.

بدوره فإن مزود الإنترنت الرئيسي في الدولة سوف يقوم ببث هذه الإشارات إلى العالم ولكن على الأغلب ليس بطريقة لا سلكية بل عبر كيبلات الإنترنت، أي الأسلاك التي تربط مزودات الإنترنت في دول العالم بعضها ببعض.



مزود الإنترنت الرئيسي يخضع لحراسة أمنية مشددة وإجراءات صارمة حيث أنه الباب الوحيد الذي يوصل الإنترنت في دولة ما مع بقية العالم، ويرتبط مع بقية العالم من خلال الكيبلات.

- ولكن من ماذا يتكون برج الإتصال نفسه؟

برج الإتصال هو مثل الراوتر بالضبط (بالمفهوم البسيط)، ولكن راوتر عظيم جداً يمكنه استقبال ترليونات البيانات وإعادة بثها.

لذلك كما يمكن اختراق الراوتر المنزلي بالتالي يمكن اختراق البرج، بل ويمكن زراعة أنظمة تجسس عليه.

وهنا سوف تطرح مثال مدينة إدلب المحررة في سوريا حيث أنها أكثر مدينة يمكننا ايضاح خطورة الابراج الغير قانونية بها، فجميع خدمات الإنترنت في إدلب تمر عبر أبراج غير قانونية.

فهمنا الآن أن كل الإشارات اللاسلكية والسلكية يجب أن تنتهي في مكان واحد وهو مركز الإنترنت الرئيسي في الدولة، فلو كان لديك ألف برج في النهاية كلها ليست أكثر من عملاء لهذا المركز وضيفتها هي إيصال البيانات له، وهذا المركز هو من يبث إشارتك خارج الدولة لأنه هو من يملك القدرة والصلاحيات للوصول إلى كيبلات الإنترنت الرئيسية او إلى موجهات الأقمار الاصطناعية التي يمكن من خلال بث الإشارة خارج الدولة. يعني لديه مفاتيح الأبواب.

وحتى تمتلك هذه القدرات أنت بحاجة لتصاريح دولية وهذه التصاريح لا يتم منحها لكل من هب ودب، حيث يجب ان تكون دولة بحكومة معترف بها دولياً، متواجدة ومعترف بها في الجهات الدولية المختصة.

مثلا حتى تتمكن من الحصول على ايبيهات IPs خاصة بك لابد لك أن تكون معترف بك كدولة في ال ICANN

Internet Corporation for Assigned Names and Numbers (ICANN)

مؤسسة الإنترنت للأسماء والأرقام المخصصة

وهي من تقدم الأيبيهات واسماء النطاقات ... إلخ

إذا لم تكن مشترك بها فمن المستحيل أن تتمكن من الحصول على هذه الخدمة حتى إن كنت قد أسست حكومة ولديك منطقة خاضعة تحت سيطرتك مثل إدلب على سبيل المثال. في النهاية هذه الحكومة غير معترف بها فإن ذهبت لهم فسوف يطردوك من الباب.

لذلك في إدلب لايوجد أي خدمات محلية للإنترنت وللحصول عليها تم ابتكار وسائل اخرى عبر تركيا. وهي من خلال تركيب أبراج إتصالات خاصة على الحدود التركية تلتقط اشارة من الإنترنت التركي وتبثها عبر أبراج أخرى عبر مناطق المحرر.

فإذا دخلت الإنترنت من إدلب فأنت بالنسبة للعالم غير موجود في إدلب بل موجود في تركيا، فآخر برج معترف به دولياً موجود في مدينة تركية حدودية مثلا ومنه يتم بث البيانات واستقبالها عبر أبراج غير معترف بها لا تتبع لشركة اتصالات معترف بها في تركيا.

وهذا السبب أنك إذا فحصت عنون الآي بي الخاص بك فسوف يقول لك أنك موجود في مدينة أزمير التركية مثلا في حين انت جالس في مدينة إدلب !!

السبب أن آخر برج معترف به من شركة الإتصالات التركية موجود في أزمير التركية وباقي الأبراج التي تمر منها الإشارة كلها أبراج شخصية أو محلية، قد تتبع لشركات تركية تعمل بلا تصاريح من هيئة تنظيم الإتصالات التركية.

هذا يعني شيئين....

الأول: جميع هذه الأبراج التي تعمل بصورة غير قانونية فهي لا تخضع للرقابة الأمنية اللازمة من قبل الحكومة التركية مثلاً.

ففي حين تفرض هيئة الاتصالات التركية قوانين صارمة وتقوم بحماية هذه الأبراج بنفسها بالبرمجيات اللازمة ومنع وصول أي شخص إليها والعبث بها، فإن هذه الأبراج الغير معترف بها والتي تعمل بما يشبه سوق سوداء للأبراج غير خاضة لهذا ابداً، أي أن صاحب البرج أوالفني الذي عمل على تركيبه ويعمل على صيانته يمكنه بكل سهولة فعل كل ما يريده دون أي ضوابط او مراقبة.

فيمكنه زراعة برمجيات تجسس وأجهزة تجسس وكل ما يخطر على بالك.

تخيل أن شخص يجلس في مدينة إدلب إن دخل الإنترنت وفحص عنوان الآي بي الخاص به قد يأخذه إلى مدينة إسطنبول التركية !!

ماذا يعني هذا؟ فمن إسطنبول إلى إدلب تحتاج عشرات الأبراج لنقل الإشارة وكلها أبراج غير نظامية وغير معترف بها في هيئة الاتصالات التركية !!

في بعض الأحيان قد يشير الآي بي إلى مدينة أنطاكيا مثلاً، هنا فآخر برج نظامي معترف به موجود على الحدود في مدينة أنطاكيا، هذه الشبكة أكثر اماناً من الشبكة التي بدأت بأبراج غير نظامية من اسطنبول بالطبع.

حسناً ماذا إن قال لك الأي بي أنك موجود في مدينة إدلب في سوريا !

- هل هذا يعني أن إدلب لديها إنترنت خاص بها ؟

لا هذا يعني أن معلوماتك كلها تذهب إلى النظام السوري...

لأن الجهة الوحيدة في هذا العالم المصرح لها فرز الأراضي السورية وتقديم أيبيهات لكل قرية او مدينة هو النظام السوري فقط، بما في ذلك إدلب وشمال حلب، لأنه دولياً فإن حكومة النظام السوري هي المعترف بها والمصرح لها تقديم الإنترنت لهذه المنطقة فقط.

لهذا فإن الأبراج القادمة من تركيا لا يمكنها تخصص أيبيهات خاصة بإدلب، فليس لديها التصاريح اللازمة، ولكن هذه التصاريح موجودة بطبيعة الحال عند النظام السوري فقط.

بالتالي إذا فحصت الآي بي الخاص بك وقال لك أنك في مدينة إدلب – سوريا فهذا يعني أن بياناتك تنتقل عبر الأبراج لتنتهي كلها في دمشق.

وهذا موجود فعلاً في إدلب حيث هناك شركات إتصالات تأخذ الإنترنت كله من النظام السوري، أي كمن تقدم بيانات الأنترنت في المناطق المحررة كلها هدية للنظام السوري على طبق من ذهب .

أي شركة إتصالات ، عراقية، هندية، ماليزية، فنزويليه، أختر أي دولة للشركة تحب إن أعطتك آي بي سوري فهذا يعني أن بياناتك سوف تنتهي في النهاية في دمشق.

إن اعطتك آي بي تركي يعني انها سوف تنتهي في تركيا وهكذا.

ولكن قبل أن تنتهي في دمشق وتركيا، فإنها قد تتعرض للسرقة والقرصنة عبر الأبراج الغير نظامية ، فهذه الأبراج لا تخضع للرقابة ولا لقوانين هيئة الإتصالات، بالتالي يمكن للفني العامل على البرج أو الجهة المشغلة له زراعة كل أنوع برمجيات وأجهزة التجسس فيه.

من الجيد أن تعلم ان الدول تحترم قوانينها...

على سبيل المثال فإن دولة مثل تركيا من المستحيل ان تسمح بان يتعرض برج نظامي يتبع لها للقرصنة، هي في النهاية سوف تجمع كل هذه المعلومات في مركز الإنترنت الرئيسي بطبيعة الحال أي انها سوف تذهب لها بكل الأحوال.

ولكن هذه الأبراج الغير نظامية ؟!! حدث ولا حرج

هذا قد يفسر لك سبب وجود أبراج غير نظامية بين اسطنبول وإدلب!!!

لان عمليات القرصنة على الإنترنت في المحرر هي عمليات كلها تتم خارج اطار القانون.

ولكن بالطبع ليس بعيداً عن نظر أجهزة المخابرات في تلك الدول.

وعليه فإننا ننصح أهلنا في مدينة إدلب بتوخي الحيطة والحذر من أي شبكة تنقل بياناتهم إلى دمشق المحتلة من النظام السوري النصيري، فجميع هذه الأبراج لم توجد إلا لتقديم بياناتكم هدية لهذا النظام.

كيف يمكنك معرفة هذا؟

ابحث في جووجل عن عنوان الأي بي الخاص بك مثلا الموقع التالي

/https://www.iplocation.net

وتأكد من دولتك

هام: بما يخص إدلب تحديداً وبعد سؤال عدد كبير من الإخوة فقد بدأ مؤخراً يظهر شبكة إنترنت إسرائيلية تستخدم بعض أنواع التخفي في الأبراج لتبدو أنها شبكة تركية، إلا أنه يمكن كشفها في بعض الأحيان، كانت التأكيدات مكررة أن هناك شبكة إنترنت إسرائيلية تم إدخالها إلى إدلب برعاية رسمية.



ربط تيليجرام سطح المكتب أو تيليجرام ويب عبر مسح رمز QR.



لتسجيل الخروج من جميع الأجهزة عدا هذا الجهاز

لقطة شاشة حقيقة لتطبيق التلجرام لجهاز متصل من إحدى شبكات الإنترنت من داخل إدلب مدعومة بشكل رسمي من الجهات المختصة في المدينة.

لايمكن كشفها بسهولة إلا أن غطاء الحماية ينكشف عنها في بعض الأحيان

حالياً يمكن كشف هذه الشبكة الإسرائيلية ببعض الطرق يمكن للجميع فعلها.

- إذهب إلى تطبيق التلجرام ثم إعدادت الخصوصية ثم عرض الجلسات، أنظر إلى أسم الدولة أسفل جلستك (قد تظهر إسرائيل في حال كنت تستخدم شبكة إسرائيلية دون أن تعلم)
- لن تتمكن من دخول عناوين كشف الأي بي كلها عبر الإنترنت لفحص الأي بي الخاص بك (أكتب في جووجل My Ip Address) وحاول دخول مواقع كشف الأي بي الخاصة بك، أشهرها وأفضلها محجوب ولن تسمح لك الشبكة بالولج إليه.
- ابحث في جوجل عن (VPN Detection أو Proxy Detection) مثلا هذا الموقع ipinfo.io شاهد تحليل معلومات الأي بي الخاص بك إن ظهر بها أن vpn أو proxy فعال في شبكتك وأنت لا تستخدمه فعندها قد يكون هذا مؤشر على وجود غطاء مزيف من قبل الشبكة لإخفاء دولتها الحقيقية أو برمجيات خاصة لإعادة توجيه البيانات.
- بعض المواقع التي تتعرف على الآي بي سوف تتعرف عليك تلقائياً أنك في إسرائيل، استمر بالبحث عن مواقع كشف الآي بي العام الخاص بك وجرب أكثر من موقع حتى تتأكد أن الشبكة غير إسرائيلية.

- كيف ولماذا تدخل شركات تتبع للنظام السوري وإسرائيل إلى مدينة إدلب وتسرق بيانات المستخدمين كلها؟

هذه الشركات تدخل كلها بتفاهمات وتصريح رسمي مع الجهات المعنية داخل البلد أو المدينة من خلال دفع مبالغ مالية طائلة تحت شعار ترخيص أو تصاريح عمل.

التبرير الوحيد لوجودها هو سرقة البيانات والتجسس ومراقبة المستخدمين.

- هل يمكنني الإرتباط بالإنترنت بدون الأبراج؟

نعم هذا نسميه الإنترنت الفضائي وهو أن تخرج الإشارات من هاتفك او راوترك مباشرة إلى القمر الصناعي، وعلى عكس ما يشاع أنه أكثر اماناً فهذا غير صحيح .

قد يكون أكثر اماناً في عملية نقل البيانات فقط، ولكن أنت تقدم نفسك كلك بجسدك هدية للقمر الصناعي لأنه سوف يكون قادر على تحديد مكانك بالسانتي متر الواحد.

فضلاً عن أن هذا النوع من الإتصالات لا يستخدم إلا من قبل محطات التلفزة والأخبار وعلى نطاق مختلف ضيق جداً، فكل من يستخدمه عليه علامات سؤال، من هو هذا؟!



في الإنترنت الفضائي فإن الراوتر يرتبط بشكل مباشر مع القمر الاصطناعي مجاوزاً كل نقاط التوزيع في العالم، وهو أكثر اماناً بالتأكيد ولكنه مثير للريبة حول هوية مستخدميه، كما يمكن تحديد موقع المستخدم بدقة متناهية.

الحماية من التتبع والمحاكيات وطبقات الحماية

إن تم إختراق جهازك، فلن تنفعك أغلب وسائل الحماية المتبعة.

وذلك لأن المخترق سوف يقوم بفتح باب خلفي (منفذ خلفي أو بورت خاص) داخل جهازك سوف يقوم بسرقة معلومات الجهاز وكل ماتفعله قبل أن يتم تشفيره من الأساس ويرسل نسخة منه إلى المخترق، كذلك سوف يستمر بمتابعة عناوين الآي بي الخاصة بك العامة والخاصة ويرسل تحديثات مستمرة لها، فأغلب وسائل الحماية لن تكون مفيدة في هذه الحالة. لذلك فإننا ننصح بحماية جهازك أولاً.

- كيف أحمي جهازي أولاً؟

ليس من السهل حماية جهازك الشخصي، بالتأكيد مطلوب منك تركيب برمجيات الحماية من الفيروسات، والجدار الناري لمنع الاختراق، تطبيقات الفي بي ان لإخفاء "الاي بي" وفحص البورتات أو المنافذ باستمرار مع إغلاق ومنع مرور البيانات من الغير مستخدم أو المشبوه منها.

ورغم هذا كله يمكن اختراق الجهاز، فالعدو متقدم تقنياً للغاية.

أول توصية نوصي بها هي عدم استخدام جهاز من الأصل، التوقف تماماً عن استخدام الهواتف النقالة، واستبدالها بأجهزة اللابتوب مع استخدام محاكيات الجوالات.

الأجهزة يجب ان تكون بمعالج قوي وبنفس الوقت صغيرة الحجم يمكن حملها بسهولة، والأهم هو مع عدم وجود كميرا داخلها وعدم وجود نظام المواقع الجغرافية "الجي بي أس".

هذه الأجهزة متوفرة بالسوق، يكفي ان تطلب جهاز بمواصفات محدده، بدون كميرا وبدون جي بي أس، ولعدم إثارة شكوك البائع اقرأ جيداً مواصفات الجهاز واحرص على أن لا يكون من بينها نظام التتبع الجغرافي ولا الكاميرا.

وفي حال تعذر الحصول على جهاز بدون كميرا، يمكن تغطيتها ببساطة بالطريقة التقليدية، بينما لا تقتني ابداً جهاز مدمج فيه نظام التتبع الجغرافي "الجي بي أس".

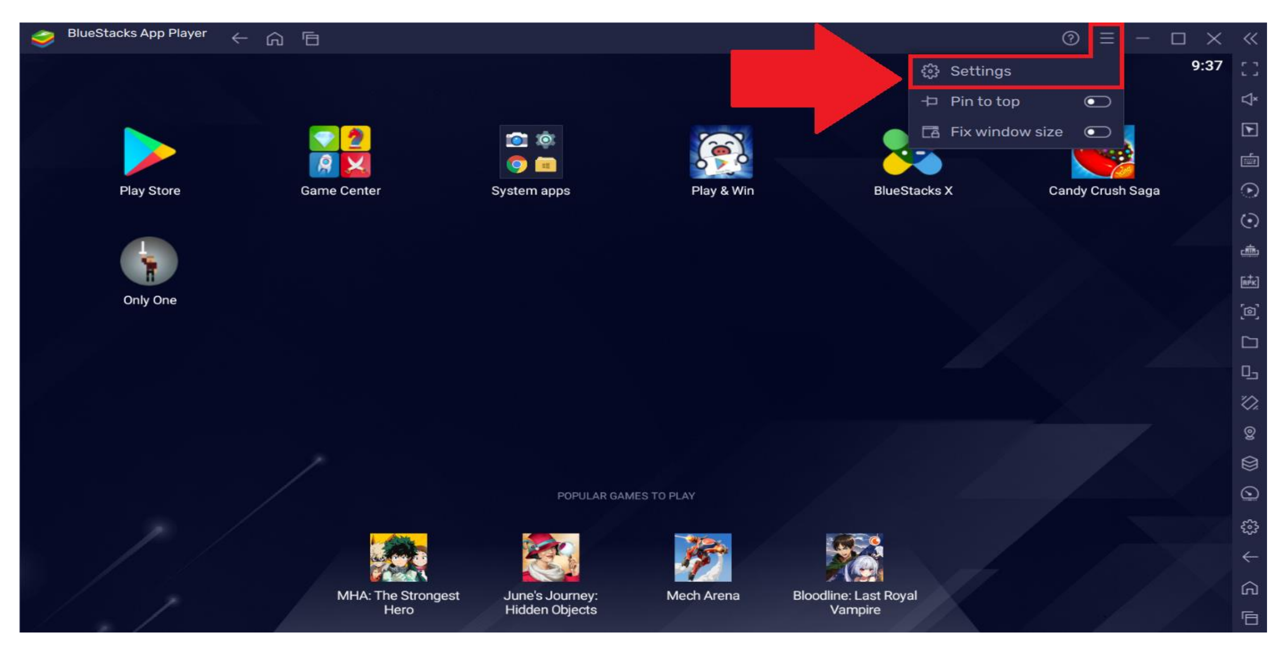
- كيف سوف استخدم تطبيقات الهاتف الجوال من خلال اللابتوب؟

لا تستخدمها مباشرة، فالتلجرام وجميع التطبيقات تقدم نسخة لنظام تشغيل ويندوز أو باقي أنظمة تشغيل اللابتوبات، ولكن لا تستخدمها.

عليك استخدام محاكيات الجوال...

وهي تطبيقات برمجية تقوم بتحميلها على اللابتوب، تسمح لك بعمل أجهزة خلوية وهمية في جهازك، بالعدد الذي تريده.

على سبيل المثال المحاكي التالي BlueStacks x
https://www.bluestacks.com
من أكثرها شهرة، ولكنك غير ملزم باستخدام هذا المحاكي تحديداً، يمكنك البحث عن بديل له.



يمكنك من خلال محاكيات الجوال عمل أي عدد تريده من الهواتف الوهمية داخل جهاز الكمبيوتر الخاص بك متجاوزاً كل المخاطر المترتبة على استخدام الهاتف التقليدي

بعد عمل الهواتف الوهمية في جهاز اللابتوب سوف تنتقل حماية اللابتوب إلى الهواتف الوهمية تلقائياً، أي أن كل مكافح فيروسات وبرنامج في بي أن تستخدمه فهو سوف يحمي اللابتوب بما فيه المحاكيات.

حيث بالطبع ستكون قد قمت بتركيب مكافح الفيروسات، الجدار الناري، الفي بي أن، حماية الشاشة.

وبشكل تلقائي سوف تعمل حماية اللابتوب على حماية الهواتف الوهمية.

ولكن كطبقات إضافية للحماية، يمكنك التعامل مع الهاتف على أنه غير وهمي، وقم فيه بتركيب مكافح فيروسات، وجدار ناري، وفي بي أن وحامي شاشة خاص به.

الأمر جيد، كلما قمت بتركيب طبقات حماية أكثر فهذا أفضل. بالطبع يعتمد على سرعة معالج اللابتوب ومواصفاته بالإضافة لسرعة شبكة الأنترنت عندك.

وبالطبع بت تدرك الآن أن تطبيق الهواتف الوهمي هو بحد ذاته طبقة حماية إضافية.

لا أريد التوصية بتطبيقات محددة، بل الأفضل أن يقوم جميع الإخوة بالبحث بأنفسهم، السبب أنهم خلال بحثهم سوف يقرأون أكثر، ويفهمون أكثر، ويتعلمون أكثر.

حسناً الآن تصور معي هذا المشهد ...

أنت تستخدم محاكي جوالات في اللابتوب، يوجد داخل الهاتف الوهمي في بي أن من شركة روسية، ومكافح فيروسات من شركة صينية، وجدار ناري وحامي شاشة.

ثم في اللابتوب نفسه تستخدم في بي أن من شركة كورية، مكافح فيروسات من شركة أخرى، جدار ناري وحامي شاشة ....

ثم أرسلت رسالة عبر تطبيق مشفر بالكامل End to End

مرحباً بك في عالم التعقيد ....

إن وقعت حزمة رسالتك هذه بيد جهة ما في العالم وكذب تطبيق التشفير وقام بفك تشفيرها، سوف يصطدم بتشفير شركة في بي أن الهاتف الوهمي، سيذهبون لها، ستفك التشفير، سوف تصطدم بتشفير شركة الفي بي أن في اللابتوب ... الخ

حسناً ماذا لو تم اختراق الهاتف الوهمي؟ سوف يصطدمون بحماية اللابتوب نفسه.

باقي الهواتف الوهمية في أمان تام.

وعليه فإننا ننصح في الهواتف الوهمية أن لا تقوم بجعل كل عملك في هاتف واحد فقط، قسمها، باختصار أجعل من سوف يوقع بك يذوق الأمرين قبل التمكن من هذا إن استطاع.

ولكن بطبيعة الحال فإن هناك نصيحة هامة لا تتجاهلها فيما يتعلق في الفي بي أن

نتصحك بالإبتعاد عن التطبيقات المجانية

هذا الأمر غاية بالضرورة، خصوصاً في مكافح الفايروسات والجدار الناري والفي بي أن.

استخدموا التطبيقات الرسمية المباعة، واختاروا تطبيقات من شركات ودول مختلفة كما ورد شرحه سابقاً، وادفعوا ثمن الخدمة من خلال العملات المشفرة "البتكوين".

- ليس لدي لابتوب، لا يمكنني الحصول عليه الآن، هل يوجد بديل للمحاكيات مخصص للهواتف؟

نعم يوجد ولكن ليس بنفس القوة والكفاءة، سوف يتم شرحها.

- ماذا لو سقط جهازي بيد العدو؟

هنا تأتي مرحلة الإبتكار. حيث يمكنك ابتكار طرق حماية إضافية.

شخصياً لا أوصي أبداً أن تكون جميع ملفاتك على اللابتوب، بل يكون جهاز اللابتوب مجرد وسيلة فقط.

بينما تقوم بتركيب تطبيقات الهواتف الوهمية وكل ما يلزمك من تطبيقات أخرى على ذاكرة خارجية "فلاش مثلاً" بسعة عالية جداً 1 تيرا بايت مثلا أو 500 جيجا.

وبمجرد سحب هذا "الفلاش" من الجهاز فعندها يصبح فارغ بلا فائدة لأي جهة كانت.

والجميل في هذا الأمر أن بمقدورك أن تعود وتستخدم هذا "الفلاش" في أي جهاز آخر.

بالطبع الذاكرة الخارجية لابد أن تكون محمية بنظام تشفير، لذلك عند اختيارها اختر نوع الذاكرات الذي يكون محمي بكلمة مرور، او قم بتركيب نظام تشفير عليها.

في أسوأ الأحوال، إذا تعرضت للمداهمة، كل ما يلزم الأمر هو إخراج "الفلاش" في ثانية واحدة ثم تكسيرها أو رميها في مكان يصعب الوصول إليه.

- هل من إجراءات اضافية؟

بالطبع، الحماية عالم لا ينتهي، والابتكار هو مفتاح النجاح بها.

قد يأتي أخ الآن ويستنبط ويبتكر فكرة جديدة من الشرح أعلاه تقوي من بروتوكولات الحماية هذه.

مكافح الفايروسات والجدار الناري

الحقيقة الصادمة حول إختراق الأجهزة هي أنه لا توجد أي طريقة في العالم تمكنك من التأكد يقيناً أن جهازك غير مخترق، لهذا عليك الإفتراض دائماً أن الجهاز مخترق وتتخذ الإجراءات التي تمنع المخترق من الوصول إلى أي بيانات.

- مكافح فايروسات
- جدار ناري
- في بي أن تشفير
- مانع تصوير الشاشة
- المحاكيات
- طبقات الحماية داخل المحاكيات
- برمجيات التشفير العامة والخاصة
- استخدام المنصات الموثوقة والمشفره End to End

هذه كلها وسائل لحماية البيانات وحايتك من الإختراق حتى إن حدث سلفاً.

ولكن بشكل عام يمكنك أن تعرف بوجود اختراق إن وجدت عملية خروج للبيانات من جهازك غير مصرح بها.

غالباً هذه مهمة الجدار الناري الذي سوف ينهبك لها كذلك ومكافح الفيروسات بالطبع لذلك احرص دائماً على اختيار الأفضل.

حالياً فجميع برامج مكافحة الفايروسات الموثوقة والمدفوعة بالطبع تقدم لك خدمات كاملة لحمايتك من الإختراق مثل الجدار الناري، وتعمل على تحديث نفسها باستمرار وفحص جهازك بصورة دورية كذلك وفحص أي ملف جديد تقوم بتحميله في الجهاز.

لذلك لا تستهين ابداً بأهمية مكافح الفايروسات بل وبأهمية شراء نسخة مدفوعة كاملة منه وعدم الإعتماد على النسخة المجانية فقط.

فمكافح الفايروسات يعتبر طبقة حماية إضافية هامة للغاية، لا تستخدم الإنترنت بدونه.

في 1% من الحالات لن يتمكن الانتي فايروس من اكتشاف البرمجيات الضارة، وهنا نحن نتكلم عن برمجيات تم برمجتها من قبل فرق مختصة على الأغلب هي فرق حكومية تمكنت من التحايل على الانتي فايروس.

لذلك فإن اتباعك لسبل الحماية التي تم شرحها في هذه الدروس سوف يحميك بإذن الله تعالى حتى من ال 1% المتبقية.

الدراسة التالية تقدم لك أفضل أنواع الأنتي فايروس التي يمكنها استخدامها

https://cybernews.com/best-antivirus-software/antivirus-for-windows-11

أو يمكنك البحث بنفسك عن مواصفات البرامج والخدمات التي تقدمها.



يعمل مكافح الفيروسات والجدار الناري على كشف أي برمجيات خبيثه وحماية جهازك من الإختراق

الأرقام الوهمية

- سمعت كثيراً بمصطلح الأرقام الوهمية فما هو الفرق بينها وبين الأرقام الحقيقية؟

يعتقد الكثير من الناس أن أهمية الأرقام الوهمية تنحصر في الحصول على رقم بدون اسم حقيقي وبدون الحاجة لإبراز وثيقة إثبات الشخصية، إلا أن أهميته تتجاوز هذا القدر بكثير.

عندما تقوم بوضع شريحة هاتف SIM Card في هاتفك الجوال فإن أول ما تفعله هذه الشريحة هو الحصول على رقم IMEI الخاص بجهازك، وهذا هو رقم فريد لا يتكرر لجهازين في العالم ابداً، إن وقع بيد أجهزة المخابرات الدولية فعندها عليك حرق الجوال والتخلص منه فوراً، لأنه لن ينفعك بعدها التخفي ابداً.

ليس فقط شريحة الهاتف هي من يمكنها الحصول على رقم IMEI بل حتى جميع تطبيقات الجوال التي تقوم بتحميلها من المتجر أو غير المتجر، مثل تطبيق التلجرام أو واتس أب أو غيرها من التطبيقات.

فإذا مثلاً قمت بوضع شريحة جوال داخل الهاتف، فعلت بها تطبيق التلجرام ثم قمت بالتخلص من الشريحة، هنا قد تظن أنك في أمان من أي خطر يتعلق بالشريحة! وهذا غير صحيح، فقد تم رصد رقم IMEI الجهاز الخاص بك ومعرفة أن مستخدم هذا الجهاز هو من استخدم الشريحة الفلانية يوماً ما، عندها إن قمت بعمل حساب تلجرام جديد من شريحة مختلفة فلن ينفعك هذا التخفي شيء، لأن رقم IMEI هو نفسه لا يختلف.

تقاطع المعلومات وكسرات الخبر التي تتركها خلفك بلا مبالاة خطر حقيقي فلا تتجاهله

على سبيل المثال يتواجد في منطقة إدلب السورية شركة هواتف رسمية، تقدم لك شريحة جوال بسعر 1 دولار فقط، يمكنك تفعيل كل أنواع البرامج عليها، وكذلك يمكنك الحصول على شريحة جديدة في أي وقت إن فقدت شريحتك الأصلية.

في الوقت الذي قد يصل به سعر الرقم الوهمي الواحد إلى دولار أو نصف دولار لتفعيل برنامج لمرة واحدة فقط، فإن هذه الشركة تقدم لك خدمة كاملة برقم رسمي وإنترنت وكل الميزات الكاملة بسعر فقط 1 دولار أمريكي!

حسناً فكر، 1 دولار فقط فما هو مكسب الشركة؟

نعم بالضبط، المكسب هو معلومات وبيانات، كما ذكرنا سابقاً حول تطبيقات الفي بي أن المجانية، الهدف دائما هو أنت، فأنت السلعة.

لذلك فإننا ننصح دوماً باستخدام الأرقام الوهمية، وذلك لأنك باستخدامها فإنك لا تحصل فقط على رقم بدون اسم ولكنك سوف تحصل على ميزات الآمان التالية جميعها.

- عدم ارتباط الرقم بشخصيتك الحقيقة
- عدم وجود شريحة وبالتالي استحالة معرفة IMEI الجهاز من خلاله أو التجسس عليه
- الأرقام الوهمية تنتقل بين الناس سريعاً، فإن امتلكت رقم اليوم ثم تركته فعلى الأغلب سوف يستخدمه شخص أخر بعد وقت قريب للغاية وهكذا كان قبل استخدامك له، لذلك فسوف تجد على الرقم الواحد عشرات ومئات حسابات التطبيق نفسه التي تم ويتم تفعيلها باستمرار، بينما الشريحة تدخل مرحلة حذف قد تصل إلى 6 أشهر أو سنة كاملة قبل حصول شخص غيرك على نفس الرقم بعد تركك له.
- سهولة ومرونة تبديلها وامتلاكها فيمكنك الحصول على عشرات ومئات الأرقام الوهمية دون تعقيد ودون الحاجة لمغادرة كرسيك أو تبديل شرائح.
- سوق الأرقام الوهمية هو سوق لا مركزي، فلا يوجد جهة في العالم يمكنها السيطرة عليه.
- يمكنك شراء هذه الأرقام باستخدام العملات الرقمية المشفرة.
- يمكنك اختيار أي دولة في العالم فلا يمكن حصرك ضمن نطاق جغرافي محدد.
- بعض أنواع هذه الأرقام تسمح لك باستقبال الرسائل المتعددة بل وحجز الرقم لفترة زمنية واستقبال المكالمات الصوتية عبر النت.

- كيف تعمل الأرقام الوهمية؟ هل تديرها أجهزة مخابرات؟

للإجابة على هذا السؤال لا بد أن نفهم آلية عمل هذه الأرقام، فهي تشبه إلى حد كبير عمل الإنترنت نفسه اليوم وحتى عمل العملة الرقمية المشفرة مثل البتكوين وباقي العملات اللامركزية .

إن سوق الأرقام الوهمية هو سوق لا مركزي ينشط في الإنترنت المظلم (الديب ويب) يديره أشخاص مختلفين لأغراض تجارية، ولا نتحدث عن أشخاص معدودين بل جميع الناس يمكنهم بيع الأرقام الوهمية في الديب ويب، ويوجد عشرات الآلاف من الأشخاص حول العالم يفعلون هذا بالفعل.

حيث يمكن لأي شخص أن يقوم بشراء أجهزة ومعدات خاصة تسمح له بتركيب ألف شريحة جوال مثلاً وربطها مع موزع أرقام وهمية في الديب ويب والحصول على مبلغ مالي مقابل كل رسالة تفعيل تصل لأحد هذه الأرقام.

فرقمك الوهمي الذي قمت لتوك بتفعيل تطبيق التلجرام عليه قد يكون مالكه هو شاب في جنوب أفريقيا لديه عشرات ومئات الأرقام الأخرى بعيداً عن بيته الآن ويتقاضى المال مقابل رسائل التفعيل بشكل آلي.

إن هذا السوق اللامركزي يؤمن لك الحماية الإضافية، فلا يمكن لأي جهة بالعالم أن تسيطر عليه بالكامل ولا حتى على أجزاء منه، إنه يشبه كثيراً السوق اللامركزي للعملات الرقمية المشفرة.

- كيف يمكن الحصول على كميات كبيرة من الأرقام الوهمية بسعر أرخص؟

إن كنت مستخدم عادي تشتري الأرقام الوهمية عبر تطبيقات ومواقع الأرقام فغالباً فإنك سوف تصطدم بسعرها المرتفع! الذي قد يصل في بعض الأحيان وبعض الدول إلى أكثر من دولار، ويتراوح بين 20 سنت و 5 دولار بل و 10 دولار احياناً لرسالة التفعيل الواحدة!

فماذا لو كنت تود تفعيل 10 أرقام يومياً؟

عملنا في الجهاد الإعلامي يحتاج الكثير والكثير من هذه الأرقام!

لايمكننا تحميل هذه الميزانية العالية بالتأكيد!

لذلك عندها عليك تجاوز هذه البرامج والتطبيقات والتعامل بشكل مباشر مع مزودين هذه الخدمات عبر الديب ويب والحصول على الأسعار التنافسية، والذين لايمكن التعامل معهم إلا برمجياً فعندها عليك أن تمتلك برمجياتك الخاصة التي تخولك الدخول إلى هذا العالم المظلم نفسه.

أو استخدام النوع الثاني من الأرقام وهي الأرقام الوهمية الغير مشروعة إن صح التعبير، حيث تعمل فرق مختصة في الإنترنت المظلم على التحايل من خلال إنشاء أرقام تبدو حقيقة بالكامل وبيعها بأسعار أرخص، هذه الأرقام غير مضمونة دائما فقد تواجه رسالة من التطبيق يقول لك هذا الرقم غير حقيقي أو هذا الرقم لا يصلح! لكنها تستحق التجربة والمحاولة نظراً لسعرها التنافسي.

أخيراً، هذا السوق لا مركزي في كل شيء بما فيه الأسعار وينطبق عليه مبدأ العرض والطلب.

فكلما زاد الطلب على رسائل تفعيل تطبيق معين سوف يزيد سعر هذه الرسائل، وكلما قل الطلب سوف يقل السعر.

لذلك فإننا ننصح المجتمع الجهادي الإلكتروني بتبديل التطبيقات باستمرار والبحث عن أكثرها أماناً وهذا ماسوف يتم شرحه في باب تطبيقات التواصل المشفرة.

تطبيقات الجوال والمواقع الإلكترونية

بالتأكيد سمعت عن الفرق الشاسع في الأمان بين استخدام موقع إلكتروني وتطبيق للجوال او حتى برنامج للكمبيوتر!

قد تطرقنا في فصل سابق إلى خطر رقم IMEI الجهاز، وكما يمكن لأي تطبيق يتم تحميله إلى هاتفك الجوال الحصول على هذا الرقم فإن بامكانه فعل الكثير مثل فتح باب خلفي لإختراقك من خلاله والتجسس على بياناتك ومعلوماتك.

لذلك فإننا ننصح الجميع بتجنب تحميل وتركيب تطبيقات الجوال الغير موثوقة عالمياً والغير موصى بها من قبل فرق الحماية والأمن الرقمي العالمي المختلفة.

ولكن ماذا عن الموقع الإلكتروني؟ هل ينطبق عليه هذه القواعد؟

بالتأكيد لا، فلا يمكن للموقع الإلكتروني الذي تستخدمه عبر المتصفح أن يحصل على أي من هذه البيانات الخاصة بك، كما لايمكن إختراق الجهاز من خلاله مالم تقم طواعية بتحميل برمجيات من هذا الموقع.

ولكن لا بد من الإنتباه من تلك المواقع التي قد تطلب منك إضافة ملحقات إلى المتصفح لديك، حيث لن يكون بمقدورك استخدام الموقع إلا بعد الموافقة على رسالة إضافة ملحق خاص بالموقع إلى المتصفح extensions حيث ينطبق على هذه الملحقات البرمجية الخاصة جميع ما ينطبق على التطبيقات من مخاطر أمنية، قم دوماً بفحص الملحقات في متصفحك extensions chrome والتأكد من خلوها من أي ملحقات لمواقع إلكترونية لا تعلم عنها ولم تصرح بها، كذلك استخدم متصفحات الإنترنت الآمنة مثل متصفح Brave.

واحرص دوماً على إجراء بحث واسع حول أي تطبيق أو متصفح تستخدمه خصوصاً تلك المتصفحات التي تقدم لك خدمات البروكسي والتخفي، تحقق من تبعيتها وحقيقة مشغليها.

- كيف اعرف أن الموقع الإلكتروني آمن للتصفح؟

بما أن الموقع الإلكتروني الذي تستخدمة لا يطلب منك تحميل أي ملفات إلى جهازك أو أي ملحقات للمتصفح فهو آمن تماماً على جهازك من الإختراق.

ولكن ما زال هناك بعض المعلومات التي يمكن للموقع الحصول عليها، مثل نوع المتصفح أو عنوان الآي بي الخاص بك.

ولتجنب هذا عليك دوماً الحرص على استخدام وسائل الحماية التي تم شرحها في هذه الدروس.

فالمتصفح آمن تماماً من هذه الناحية، أي أنه لا يمكن للمتصفح أن يخترق هاتفك، مستحيل وقطعياً . ولكن يمكنه مثلا معرفة معلومات معينة مثل الآي بي الخاص بك ، نوع المتصفح الذي تستخدمه، وبعض الأمور التي لا تهدد أمنك بشكل مباشر ، وهذا ليس بالضرورة أي أن هذا يعتمد على الموقع الإلكتروني نفسه فيمكن لمدير هذا الموقع رفض استقبال عنوان الآي بي الخاص بك.

في بعض المواقع يتم استخدام الخدمات السحابية، أشهرها هو

https://www.cloudflare.com

فعندما تطلب عنوان الموقع يتم أولاً تحويلك الى موقع الكلاود هذا ثم من خلاله تخرج البيانات مشفره وتعود إليك مشفره، هو بمثابة البروكسي أو الفي بي أن للمواقع.

ومن ميزاته كذلك أنه يخفي هويتك أنت أي هوية الآي بي الخاص بك (إن قام مالك الموقع بتفعيل هذا النوع من الحماية) فيرسلك إلى الموقع الإلكتروني بآي بي خاص بموقع الكلاود وبهوية مزيفه من الكلاود فلا يمكن لمدير الموقع نفسه معرفة تفاصيل كثيرة عنك قد يتمكن من معرفتها إن دخلت الموقع بشكل مباشرة بدون هذا الوسيط وهو الكلاود.

كيف تعرف ان الموقع يستخدم هذه الخدمة؟

ادخل هنا

https://whois.is

اكتب عنوان الموقع الإلكتروني الذي تود البحث عنه في مربع البحث مثلا google.com

سوف يعطيك معلومات تفصيلية عن هذا النطاق ، من مالكه ورقم هاتفه .. الخ

طبعا في المواقع الرسمية تكون معلومات حقيقة بينما في المواقع الجهادية مثلا كلها تكون مزوره غير حقيقة وغالباً لن تظهر لك حيث أن كثير من المواقع تطلب إخفاء هذه المعلومات.

ولكن بعض المعلومات لايمكن إخفائها ويهمنا منها هو هذا Name Server

إن أشار النيم سيرفر هذا إلى موقع CLOUDFLARE.COM أو موقع مشابه له فهذا يعني أنك قبل دخول الموقع فانك تدخل موقع CLOUDFLARE والذي بدوره سوف يقوم بتشفير إتصالك بطبقة حماية جديدة، ثم إرسالك للموقع النهائي.

يوجد استخدامات كثيرة للكلاود وفي الحقيقة فإن مدراء المواقع قد لايهم الكثير منهم حماية زوارهم، ولكن يهمهم حماية الموقع نفسه، فالكلاود يحمي الموقع من الزوار كذلك ، يحميه من الإختراق والهجمات ... الخ، هو طبقة حماية اضافية للموقع مثل الفي بي أن ، حيث أن المواقع الإلكترونية خصوصاً في الديب ويب تستخدم طبقات حماية مشابهة تماماً لطبقات الحماية الشخصية التي تم شرحها في هذه الدروس.

بالعودة إلى السؤال المهم: هل يمكن اختراق الجهاز عبر موقع الكتروني من المتصفح.

الجواب : لا

لأن الموقع الإلكتروني لا يدخل إلى نظام التشغيل الخاص بك، فبما أنك لم تقم بتحميل شيء من الموقع واكتفى تواجدك به على التصفح فقط فهذا يعني أنه من المستحيل اختراق جهازك من خلاله.

ولكن عليك الإنتباه جيداً إلى اضافات المتصفح Extensions كما ورد ذكره.

بعض المواقع عند دخولها سوف يظهر لك في الأعلى في الزاوية تقول لك نود تركيب إضافة إلى المتصفح لتتمكن من استخدام هذا الموقع اسمها بالانجليزي Extensions، لا تفعل ذلك مالم تكن واثق من الموقع تماماً.

لان هذه الإضافة تعتبر مثل التطبيق، انت من خلالها سوف تعطي هذا المواقع صلاحيات واسعة في جهازك. ونعم يمكن اختراقك من خلالها.

وبالحديث عن اختراق الأجهزة من خلال الروابط لا بد لنا من الحديث عن بيجاسوس الإسرائيلي..

سمعنا أنه بمجرد إرسالهم رابط الكتروني للضحية او الإتصال معه عبر اي تطبيق لمدة 10 ثواني فقط فإنه يتم اختراقه !!

إذاً الموقع الإلكتروني يمكنه اختراق الجهاز صحيح؟

برنامج بيجاسوس لا يخترق الجهاز عبر المتصفح بل يستخدم ثغرات موجوده سلفاً في نظام التشغيل .أحدث ضجة عالمية كبيرة، وضحيته الأكبر كانت شركات مثل جووجل وأبل، حيث أنه اخترق أنظمة تشغيلها نفسها ووجد ثغرات بها.

فهو لا يعمل على زراعة شيء داخل جهازك من خلال إختراق الجهاز نفسه يفتح له باب خلفي تقليدي كما شرحنا في مشاركات سابقة، بل يستخدم ثغرات وابواب خلفية موجوده في نظام التشغيل نفسه سلفاً، عيوب في نظام التشغيل اكتشفها فريق عمل بيجاسوس .

والرابط الإلكتروني أو المكالمة الهاتفية التي تصلك هذه من أجل تهيئة عملية استغلال هذه الثغرة. بالمحصلة هو لا يفتح باب خلفي بل يستخدم باب خلفي موجود في النظام نفسه أو يزرع برمجية خبيثة تفتح له باب خلفي خاص من خلال باب خلفي موجود بالنظام سلفاً أو في التطبيق.

مثلا في حالة تطبيق بجاسوس الذي ورد ذكره سابقاً، تمكن فريق العمل من اكتشاف ثغرة في الواتس آب قاموا من خلال إجراء اتصال مع الهدف وحتى إذا لم يجيب الهدف فإنهم من خلال هذا الإتصال قاموا بتمرير برمجيات خبيثة، لأنه بات هناك نوع من تبادل البيانات بين المرسل والمستقبل وهو ما نتج عنه حالة الرنين ، إذاً يوجد تبادل بيانات ووجدوا الثغرة منها.

لذلك عليك الإنتباه بشكل عام في الوسط الجهادي من هؤلاء الذين لا تعرفهم جيداً ويتصلون عليك بسبب وبدون سبب، مثل ان يقوم معرف تجهله بعمل اتصال معك !! سوف تلغي أنت الإتصال ولن تقبله ولكن إن كان هذا الإتصال هدفه تمرير برمجية خبيثة إلى جهازك فقد مررها وانتهى الأمر.

أفهم وطبق دروس الأمن السيبراني التي تم تقديمها في هذه الدروس وسوف تكون كافية لحمايتك بإذن الله تعالى حتى من بيجاسوس.

المخاطر لا تندرج فقط على جهازك الخاص بل قد يأتيك الخطر من جهاز آخر لم تكن تتوقع أن يتم إختراقك من خلاله! وهنا لابد لنا الحديث عن أجهزة التلفاز الذكية والإرتباط مع شبكة الإنترنت من خلال هاتف أخر أو خدمة البلوتوث.

التلفاز الحديث يرتبط بالإنترنت وبالتالي يوجد إتصال بينه وبين النت ويمكن اختراقه، تنطبق عليه جميع ماتم ذكره على الهاتف من مخاطر، ولكن من هذا المهتم في معرفة برامجك التي تتابعها!! والأهم أنه غير منتشر.

ولكن الخطورة تكمن حينما تقوم بربط الهاتف الذكي مع جهاز الجوال الخاص بك. عندها من الممكن نقل هذه البرمجيات الى الجوال من خلال التلفاز.

لذلك ستكون كارثة كبيرة لو أنك مثلاً سجلت بريداً إلكتروني في التلفاز نفس الذي تستخدمه في جوالك، أو وضعت فيه تطبيق أو سجلت دخول في أي تطبيق قد يشير الى شخصيتك الجهادية.

والأفضل عدم إجراء هذا الربط مع التلفاز إن كان الأخ مستهدف على نطاق واسع.

البلوتوث قطعاً يمكن اختراقك منه وتمرير برمجيات خبيثة لا تحتاج لشرح كبير بعد ماتم شرحه حول التلفاز. أنت تعطي البلوتوث صلاحية تبادل بيانات مع هاتفك، اصبح راوتر ولكن خطير جدا حيث أن صاحب جهاز البلوتوث يمكنه مباشرة تمرير البرمجيات الخبيثة إلى هاتفك.

بشكل عام بمجرد إعطاء صلاحية لأي جهاز لتبادل البيانات مع جهازك فإنك تعرض نفسك لخطر الإختراق إن كان ذلك الجهاز يحتوي برمجيات خبيثة لديها القدرة على الإنتقال تلقائياً.

تطبيقات التواصل المشفرة

نحن بحاجة لتطبيقات التواصل لما تقدمه من مرونة وسرعة في الإداء، ولكن هذا الميزات لها ثمن باهض وقد يكون معلوماتك وأمنك وحياتك هي الثمن !

لذلك عليك تحري الدقة والمصداقية قبل استخدام أي تطبيق تواصل عبر الإنترنت.

حسب الدراسة التالية التي تم تقديمها من موقع nordvpn

https://nordvpn.com/blog/most-secure-messaging-app

لاحظ أن هذه الدراسة القيمة اهتمت ولخصت التطبيقات حسب جوانب رئيسية مثلاً

- E2E encryption التشفير ايند تو ايند
- Self-destructing messages التدمير الذاتي للرسائل
- Collects data about users and their contacts جمع المعلومات عن المستخدمين والاحتفاظ بها
- Tracks users' social media activity تتبع نشاطات المستخدمين عبر وسائل التواصل الإجتماعي
- وميزات أخرى سوف تجدها مكتوبة تحت التطبيق

علامة الزائد الخضراء تعني توصية

علامة السالب الحمراء تعني عيب

من أهم نقاط الضعف الأمنية في أي تطبيق هو تتبعه للنشاطات أو جمع البيانات، هذا يتم لغايات تجارية في كثير من الأحيان ولكنها بالطبع تعني التجسس عليك مهما حاولوا تجميل المصطلحات والتسميات.

لاحظ مثلاً تطبيق مثل سيجنال العيب الوحيد الذي تم اسناده له هو حاجته لرقم هاتف، فمثلاً استخدام رقم هاتف وهمي يجعله بلا عيوب حتى الآن.

كما أن التلجرام جيد خصوصاً في المحادثات المشفرة بالكامل، ولكن مشكلته أنه التلجرام، الخصوصية فيه لم تعد مضمونة ابداً حيث بات هدفاً لجميع الجهات المختصة بالحرب على الإرهاب.

فضلاً عن وجود تطبيقات اقوى منه بالتشفير والخصوصية أعلى وحسب الدراسة هي

Threema

Wickr

Signal

ومع هذا عندما تستخدم هذه التطبيقات وفي الأمور الغاية في الأهمية يجب عليك ان تقوم بتشفير رسائل بها عبر برمجيات تشفير الرسائل، وهذه تعتبر طبقة حماية إضافية تستخدم عادة في المراسلات الهامة.

مفهوم التشفير وبرامج التشفير الخاصة

التشفير هو عبارة عن ممارسة حماية المعلومات باستخدام الخوارزميات المشفرة.

يمكن أن تكون المعلومات غير نشطة (مثل ملف على القرص الصلب)، أو متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)، أو قيد الإستخدام (أثناء الحوسبة على البيانات).

والتشفير أنواع يمكن مثلا فك الشيفرة بعشر سنوات وممكن شيفرة أخرى فكها بمائة عام.

باختصار: كل شيفرة يمكن فكها.

هذا طبيعي لأنها بالأصل مصنعه من اجل فكها على جهاز المستقبل وإلا ما الفائدة منها إن كان يستحيل فكها؟

ولكن كل شيفرة لها مفتاح خاص لايتم فكها إلا به حتى لو لم تكن تعلم عن هذا المفتاح أنت، ولكنه موجود ويكون في خلفية التطبيق.

يمكنك ملاحظة هذا مثلا في حسابك التلجرام

إذا كنت تستخدم حساب التلجرام على جهازين فسوف تلاحظ ان جميع محادثاتك على الجهاز الأول تظهر بالكامل على الجهاز الثاني كذلك.

ولكن هذا لا يحدث في حالة الغرفة المشفرة !

لماذا؟ لأن تشفير الغرفة أي مفاتيح فك تشفيرها يكون مرتبط بجهازك الذي استقبلت او قمت بعمل الغرفة المشفرة منه، ونقصد المحادثة المشفرة، بالتالي لايمكن فك شيفرة الرسائل على الجهاز الثاني نظراً لعدم توفر مفتاح فك التشفير، بالطبع حسب تعهد التلجرام فإن هذا النوع من المحادثات المشفرة هي من نوع تشفير End to End.

ورغم هذا كله يمكن فك الشيفرة، مهما بلغت قوتها.

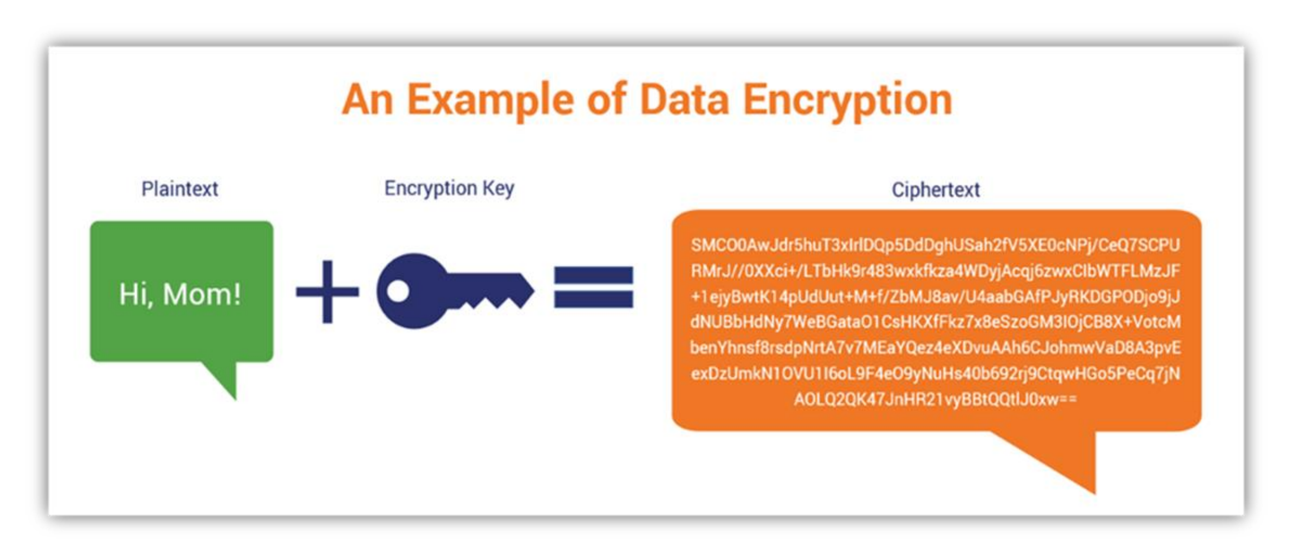
فالمسألة فقط مسألة وقت وذلك من خلال التجريب العشوائي أو مبدأ القوة الغاشمة، حيث يتم وضع النص المشفر في كمبيوتر بمواصفات جبارة، وعندها يبدأ الكمبيوتر بتجربة جميع الأرقام والرموز والأحرف الموجودة في لوحة المفاتيح بشكل عشوائي حتى يصل إلى مفتاح فك التشفير الصحيح.

مثلا لنفرض ان مفتاح فك التشفير كان هكذا 123، في هذه الحالة فإن أي جهاز حساب لن يستغرق أكثر من ثواني حتى يحصل عليه وينجح بفك الشيفرة، لأنه سهل جدا.

ولكن اذا كان هكذا sadsada@^&@@#^#^&%#& ##&#^*#^*&#^IG#JH

سوف ينجح بالنهاية بفك التشفير ولكن ممكن بعد 100 عام أو 500 عام وربما أكثر، حسب قدرات جهاز الحساب.

فما بالك أن مفاتيح فك التشفير يكون مكون من عشرات الرموز والأرقام والأحرف! نظرياً يمكن فك الشيفرة وعملياً من المستحيل ذلك.



الرسالة + مفتاح التشفير = نص مشفر يستحيل فكه إلا من خلال مفتاح التشفير نفسه

أنواع التشفير مختلفة ودرجات قوتها متباينة، بل ويمكنك عمل تشفير مركب مثلا نفرض النص التالي "مرحباً يا أخي"، تقوم بتشفيره على نظام تشفير معين، ثم تقوم بتشفير التشفير نفسه على نظام آخر ، وهكذا.

ولكن بشكل عام لا داعي لهذا إن كان التشفير قوي للغاية لأن أعظم الكمبيوترات على وجه الأرض "المعروفة" سوف يلزمها عمل مئات السنيين من أجل فك تشفير كلمة واحدة إن تم تشفيرها بأنظمة تشفير قوية.

نستخدم التشفير الخاص في حالات التراسلات المهمة مثل نقل ملف أو نص هام للغاية، فبعد اتباع جميع الإجراءات الأمنية التي تم تقديمها في هذه الدروس نقوم كذلك بتشفير المادة عبر برمجيات تشفير خاصة، ومفاتيح خاصة لفك التشفير لا يعرفها إلا الطرف الآخر.

مثال بسيط على عملية التشفير باستخدم مفتاح فك تشفير عبارة عن كلمة مرور عبر الموقع

https://www.gillmeister-software.com/online-tools/text/encrypt-decrypt-text.aspx

- اكتب النص الذي تريده، اكتب في مكان كلمة المرور أي كلمة مرور تريدها ثم اختر Encrypt.
- قم بعمل التشفير سوف يظهر لك النص المشفر في الأسفل.
- انسخ هذا النص وارسله الى صديقك والذي يعرف كلمة المرور سلفاً.
- سوف يقوم بأدخال النص وكلمة المرور ويختار Decrypt.
- وسوف يتم فك الشيفره في الأسفل.

يمكنك تشفير النص أولاً بكلمة مرور، ثم تشفير الشيفرة بكلمة مرور ثانيه

ثم صديقك عليه ان يفكها أولاً بكلمة المرور الثانية ليحصل على الشيفرة الأولى، ثم يفك الشيفرة الأولى بكلمة المرور الأولى، هذه شيفرة مركبه.

بالبحث في جووجل يمكنك ايجاد تطبيقات تشفير عالمية مشهورة ومضمونه، سوف تجدون الكثير من هذه البرامج الموثوقه لذلك فلن نوصي بأي تطبيق أو برنامج محدد، كما أن البرامج تتيح لك إمكانية تشفير مجلد بأكلمة بكل مافيه من ملفات.

حذف الملفات نهائياً مع منع استعادتها

سؤال يسأله الكثيرون، كيف يمكنني حذف الملفات من الجهاز بشكل نهائي دون إمكانية استعادتها أبداً، أو حتى كيف يمكنني التحقق من أن البرمجة الضارة التي تم إختراق الجهاز من خلالها لن تعيد تشغيل نفسها مرة أخرى بعد عمل فورمات للجهاز كاملاً؟

هل يمكن لبعض البرمجيات الخبيثة المتطورة أن تبقى مختبئة في مكان داخل الهاردسك بكامل بنيتها ثم تعيد تشغيل نفسها بعد الفورمات؟

هل يمكن استعادت الملفات بعد عمل فورمات أو بعد حذفها نهائياً من الجهاز؟

الجواب للسؤالين هو: نعم

لذلك فنحن ننصح الأخ بصورة دائمة إن لم يكن لديه خبرة كافيه بحماية نفسه أن يقوم بتغيير الجوال في حال أي شكوك حول عملية إختراق.

ولكن بإذن الله تعالى في هذ الفصل سوف نتعلم سوياً كيف نحمي أنفسنا ونتعامل مع الإختراق عبر البرمجيات، وكيف نمحي أي أثر لها ونمنعها من تشغيل نفسها بعد الفورمات، وكذلك منع استعادت الملفات المحذوفة.

البرمجيات ومنها برمجيات الإختراق كلها ترتبط مع نظام التشغيل للهاتف او بمعنى أخر هي تدخل الى القرص الصلب (الهاردسك) للجهاز.

فإذا قمت بتبديل الهاردسك او تنظيفه تماماً لن يعود لها أي أثر مالم يكون لديها قدرة على إعادة تشغيل نفسها، وبعض انواع البرمجيات الخبيثة المتطورة لديها القدرة على ذلك، حيث يمكنها إعادة تشغيل نفسها تلقائياً إن بقيت داخل الهاردسك ببنيتها الكاملة.

ما هو الهاردسك؟

هو وحدة تخزين البيانات، يتم التحكم به بواسطة وحدة التحكم في الجهاز فهي من تقول له ماذا يفعل.

بالتأكيد سمعت من قبل عن أن اللغة الأصلية للحاسبات هي 0 و 1 وهذه تعني فتح إغلاق، حالة ال 0 تعني مغلق وحالة ال 1 تعني مفتوح. ولا أود الخوض معكم بهذه التفاصيل الميكانيكية حول الجهاز ولكن الهاردسك تكون البيانات كلها مخزنة به على شكل أصفار وأحاد، 0 و 1. مثلا شيء كهذا 01011110011100101 لا يفهم الجهاز ولا يمكن تخزين اي شيء داخل الهاردسك إلا 0 أو 1، في الحقيقة هو لا يخزن 0 و 1 اصلاً بل يفعل شيء اخر ولكن يمكن اختزال الأمر بهذه الطريقة.

عندما تبدأ استخدام الجهاز يكون الهاردسك فارغ تماماً أو شبه فارغ ومع استخدامك له يبدأ يمتلىء بالمعلومات، ويبدأ بالكتابة على أجزاء الهاردسك ولن يعود للكتابة على الجزء الذي كتب عليه أولاً إلا بعد إنتهاء تعبئة الهاردسك كله.

هذا يعني انك عندما تقوم الأن بتحميل صورة ثم تحذفها فإنه لا يتم مسحها من الهاردسك ومازال من الممكن استعادتها بكل سهولة وهذا لأن قابلية المسح غير موجود في الهاردسك أصلاً، إنما هو يخفيها فقط ويحرر المساحة الخاصة بها للسماح بالكتابة فوقها أي وضع مادة أخرى، مما يتهيء لك أنه قد حذفها، وفي الحقيقة هو يضعها تحت بند مسموح الكتابة فوقها ثم يخفيها.

وعندما ينتهي الجهاز من استخدام الهاردسك كله سوف يعود للبداية ويبحث عن الاجزاء التي تم اخفاء ملفاتها ويكتب فوقها من جديد، وهكذا.

فمن الممكن أن تكون حذفت صورة قبل 10 سنوات ولكن حتى هذه اللحظة لم يملتىء الهاردسك الخاص بك ومازال حذفها من نوع حذف رقم 0 أي لم يتم كتابة اي شيء فوقها.

وهذا يعني أنه يمكن استعادتها بسهولة حتى إن مر عليها 10 سنوات.





في الشركات يتم تدمير الهاردسك المنتهي استخدامه وكذلك الأجهزه بهذه الطريقة، لتجنب أي مخاطر محتملة من استعادت البيانات

لهذا فنحن ننصح في حالة رغبتك بتنظيف الهاردسك ان تستخدم تطبيقات وظيفتها الكتابة على جميع أجزاء الهاردسك الغير مستخدمه، بما في ذلك التي تم استخدامها سابقاً وحذفت بياناتها.

هذه التطبيقات سوف تعمل على الكتابة مرة ومرتين وثلاثة وصولاً إلى 10 مرات وأكثر فوق الهاردسك وفقط الاجزاء الغير مستخدمة حالياً.

مما يعني استحالة استعادت البيانات المحذوفه، بما فيها البرمجيات الضارة والخبيثة مثل الفايروسات أو برمجيات التجسس، حيث سوف تعمل على اعطابها تماماً وبالتالي عدم قدرتها على تشغيل نفسها بعد فرمتت الجهاز إن كانت هذه البرمجيات تمتلك هذه القدرة.

فضلاً عن هذا فإنها سوف تعمل على تقسيم أجزاء الملفات نفسها واتلافها تماماً وتوزيعها داخل الهاردسك مما يعني استحالة أن تتمكن البرمجيات الخبيثة إن وجدت من تجميع نفسها من جديد، وبنفس الطريقة استحالة أن تتمكن أي جهة من استعادت الملفات المحذوفة بعد حذفها.

من أشهر هذه التطبيقات للجوال هو تطبيق Andro Shredder.

والذي عند تشغيله سوف يقوم بفحص جميع الأجزاء الغير مستخدمة من الهاردسك بما فيها تلك التي طلب حذف بياناتها وسوف يقوم بالكتابة فوقها مرة ومرتين وصولاً إلى 10 مرات، فضلاً عن هذا فإنه سوف يعمل على تقسيم وتفتيت هذه البيانات نفسها مما يعني استحالة تجميعها من جديد مرة أخرى من قبل المختصين أو تجميعها هي لنفسها.

لكن عليك أن تعلم أن استخدام التطبيق بكثرة سوف يقصر من عمر الهاردسك الخاص بك، لا مشكلة في هذا مقابل ما يوفره لك من أمان.

كما أن أغلب برامج الأنتي فايروس تقدم خدمة تقسيم وحذف الملفات نهائياً وتنظيف الهاردسك بالكامل تجدها تحت خيارات Shredder.

ومن أشهر برامج الأنتي فايروس التي تقدم هذه الخدمة هو برنامج bitdefender.

وهذا المصطلح File Shredder يعني حذف مع تدمير الملف في الهاردسك أي تقطيع الملف، فما يفعله بالضبط هو انه لايحذف الملف فقط بل يقطع بنيته الأصلية ويوزعها على الهاردسك ، فلا يمكن للملف أن يجمع نفسه من جديد أو أن يجد أحد أجزاءه ويجمعها سويا، فهذا بات أصعب من البحث عن إبرة في أكوام من القش وليس كومة قش واحدة.

مثلا هذا الشرح لعملية الحذف، ولكن هذا الحذف يكون لملف واحد فقط، وفي بعض أنواع الأنتي فايروس تجد هذه الميزة موجودة لكامل الهاردسك.

https://www.bitdefender.com/consumer/support/answer/2179/



تعمل برامج تدمير البيانات على تقطيعها مما يجعل من المستحيل استعادتها من جديد

وهنا لا بد من التذكير بأمر هام للغاية

عندما نقول الهاردسك فنحن لا نقصد القسم C منه والذي جرت العادة بتحميل نظام التشغيل مثل الويندوز عليه.

فإن هذه الأقسام C , D , E , F مجرد أقسام وهمية لترتيب ملفاتك، فعندما نقول الهاردسك نعني كل أقسامه، الهارد بالكامل.

- ماذا أفعل بالملفات الموجودة أصلاً على الجهاز في حالة الشك بوجود إختراق؟

اولاً عليك نقل ملفاتك المهمة والاحتفاظ بنسخة منها، بعد نقلها من الجهاز المشكوك في إختراقه إلى وحدة تخزين خارجية (فلاش) وبعد أن تكون قد طبقت جميع أساسيات الحماية وقمت بتحميل انتي فايروس موثوق ومدفوع، فعند وضع الفلاش في الجهاز سوف يطلب منك فحص الفلاش كاملة، اترك الأنتي فايروس يقوم بفحص كل ملفاتها.

ثم لا تقوم بفتح إلا الضروري منها فقط، أي لا تعيد كل الملفات إلى الهاردسك فقط ما تحتاجه منها إن لزم الأمر.

في 99% من الحالات سوف يتمكن الأنتي فايروس من اكتشاف البرمجيات الضارة وتنظيفها أو حذف الملفات نهائيا إذا فشل في تنظيفها مع الحفاظ على سلامة بنية الملف الأصلي.

لذلك من الأفضل قبل أن تقوم بفحصها أن يكون لديك نسخة ثانية منها على فلاش ثاني. هذا يحدث مثلاً أن يكون لديك ملف مهم، لكن اكتشف الأنتي فايروس برمجية ضاره ولم يتمكن من تنظيف الملف فسوف يقوم بحذفه نهائياً وتقطيعه.

عندها سوف تفقد الملف كله.

إن حدث أمر مثل هذا قم بتشغيل الفلاش على جهاز ثاني لا تستخدمه وانسخ النص الذي تريده إن كان مهم لهذه الدرجة.

في 1% من الحالات لن يتمكن الأنتي فايروس من اكتشاف البرمجيات الضارة، وهنا نحن نتكلم عن برمجيات تم برمجتها من قبل فرق مختصة على الأغلب هي فرق حكومية تمكنت من التحايل على الأنتي فايروس.

عندها لاقدر الله إن حدث هذا فسوف يحمي اتصالك وبياناتك باقي اجراءات الأمان المتبعة.

والشيء بالشيء يذكر...

لايمكننا التحدث عن خطورة الملفات مالم نعرج على ما يسمى بال Meta Data

الميتا داتا هي معلومات تكون موجود في أي ملف وأنت لا تعرف بوجودها.

فمثلاً إذا قمت بالتقاط صورة من جهازك وأنت قد منحت الكميرا صلاحيات الموقع الجغرافي، فإن إحداثياتك الجغرافية في لحظة التقاط الصورة سوف يتم تخزينها داخل ملف الصورة دون أن تعلم بذلك.

كذلك سوف يتم تخزين معلومات كثيرة مثل اسم الجهاز وقت التقاط الصورة ومعلومات أخرى قد تبدو لك ليست ذات اهمية ولكنها بالتاكيد مهمه جداً لأنها تعطي معلومات تفصيلية عن جهازك نفسه وعن الصورة لا تعلم عنها.

هذه المعلومات اسمها ميتا داتا أو بيانات الميتا وتكون موجود داخل الملف لايمكنك إظهارها ولكن يمكن إظهار جزء منها من خلال عرض تفاصيل إضافية عن الصورة بعد فتحها بالجهاز.

المعلومات الأكثر والأخطر يمكن رؤيتها من خلال تطبيقات خاصة بقراءة معلومات الميتا.

- هل هذا يعني أن كل صورة أصورها وأرسلها على التيليجرام تحتوي هذه المعلومات؟

حسناً في حالة التيليجرام ، الواتس آب، فإن هذه التطبيقات تقوم تلقائياً بإعادة هيكلة الميتا، أي حذف الميتا الأصلية وتغييرها وذلك مع تغيير دقة الصورة نفسها مثلاً. ولكن ليس كل شيء.

بينما إذا قمت بارسال ملف أو صورة عبر موقع تحميل أو عبر البريد الإلكتروني أو بأي طريقة أخرى فإن معلومات الميتا يمكن استخراجها وبالتالي معرفة كثير من الأشياء التي كنت تجهل وجودها.

- كيف يمكنك تغيير هذه المعلومات؟

ابحث في جووجل عن هذا

metadata changer

سوف يظهر لك تطبيقات وبرامج وأيضاً مواقع إلكترونية تمكنك من رفع الملف ثم تغيير معلومات الميتا ثم تحميله من جديد.

الخاتمة

إن أصبنا فإنه من فضل الله علينا وإن اخطأنا فمن الشيطان.

عالم الحماية واسع للغاية والتقنيات تتبدل باستمرار، وما هو آمن اليوم قد لا يكون هكذا غداً. لذلك فإننا ننصح دوماً بمواكبة هذا العلم وتحديث قناعات المجتمع الجهادي باستمرار حول سبل الحماية المتبعة.

تم إعداد هذا الكتاب بالتعاون مع مجلس التعاون الإعلامي الإسلامي IMCC

في حال وجود أي إستفسار أو سؤال لا تتردد بالتواصل مع إخوانك في المجلس عبر طرق التواصل المتاحة أو عبر المؤسسات المنتسبة للمجلس.

وآخر دعوانا أن الحمد لله رب العالمين

القسم التقني – الحرب الإلكترونية

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)



أفضل الاختيارات للسرعة والسعر والخصوصية والمزيد

تقديم: جيش الملاحم الإلكتروني

إعداد: مجلس التعاون الإعلامي الإسلامي



Al-Malahem Electronic Army

بسم الله الرحمن الرحيم

جيش الملاحم الإلكتروني

يقدم

*** دراسة ملحقة: أفضل خدمات VPN لعام 2023 ***

أفضل الاختيارات للسرعة والسعر والخصوصية والمزيد

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

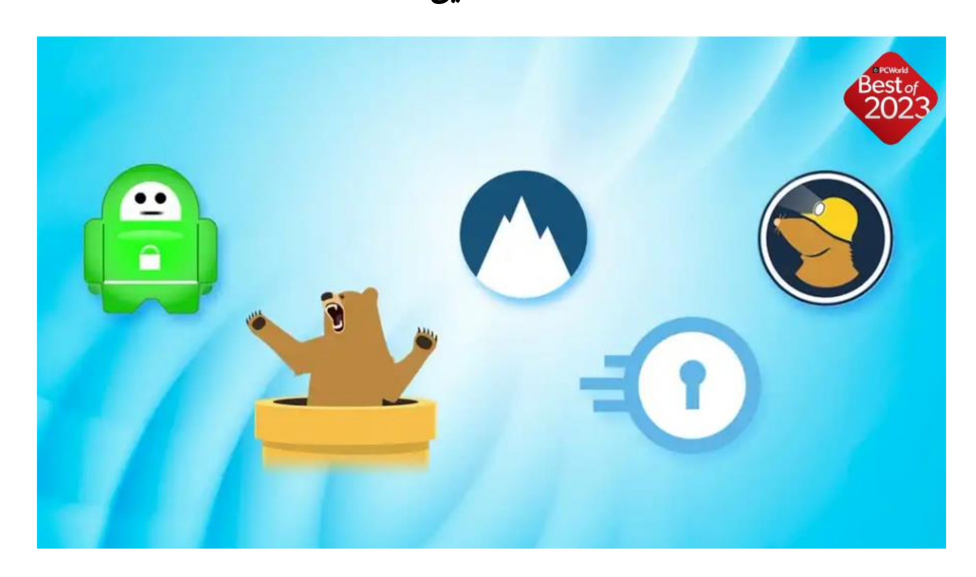
4/ 1445هـ - 11/ 2023 م

المصدر

https://www.pcworld.com/article/406870/best-vpn-services-apps-reviews-buying-advice.html

المقدمة

يمكن لخدمة الشبكة الافتراضية الخاصة، المعروفة أيضًا باسم VPN، أن تساعد في حماية هويتك وموقعك، والحفاظ على أنشطتك عبر الإنترنت وابقائها مجهولة ومحجوبة عن أعين المتطفلين.



هناك بعض الأشياء التي يجب عليك مراعاتها عند البحث عن VPN.

- يجب أن يكون قادرًا على الحفاظ على خصوصية استخدامك للإنترنت وأمانه دون تسريبات.
- السرعة مهمة أيضًا، فالخصوصية والأمان مهمان للغاية، لكنك لا تريد أن تؤثر الخدمة على سرعة الإنترنت لديك أيضًا.
- وإذا كنت مهتمًا بعدم الكشف عن هويتك، فيجب عليك البحث عن VPN مع سياسات جمع البيانات الواضحة والشفافة.
- أخيرًا، يعد عدد الخوادم المتاحة ومواقع البلدان التي تقدمها VPN أمرًا مهمًا إذا كنت تحاول تجاوز أقفال المنطقة في بلدان معينة.

التالي هي أفضل شبكات ال VPN للعلم 2023 مع الأسباب والإيجابيات والسلبيات

من الصعب اختيار أفضل VPN بشكل عام وذلك لأن بعض الخدمات أضعف فيما يتعلق بالخصوصية، ولكنها أسهل في الاستخدام بشكل كبير مع الكثير من الميزات، في حين أن البعض الآخر أكثر تعقيداً بالإستخدام ولكنه أكثر أماناً.

فالأفضل بالنسبة لك قد يكون الأكثر سهولة ومرونة وبالنسبة لغيرك قد يكون الأكثر أماناً، وبينما قد يهتم أحدهم إلى ضرورة اختيار VPN لا يحتفظ بسجلات فقد يرى الآخر أن لا ضرر في ذلك، وعليه فإنك أنت من تقرر الأفضل بالنسبة لك.

ExpressVPN

الأفضل في عام 2023

توصية IMCC: جيد



الإيجابيات	السلبيات
سرعات جيدة باستمرار	يسجل كميات نقل البيانات **(عيب خطير، ليس الأفضل للخصوصية)**
برنامج سطح مكتب سهل الاستخدام	أغلى من العديد من المنافسين
دعم واسع للجهاز	

لسنوات عديدة اخترنا أفضل VPN استنادًا إلى الخصوصية فقط، لكن هذا لم يعد الشغل الشاغل لمعظم الأشخاص عند اختيارVPN .

من المؤكد أن الخصوصية مهمة، ولكن الأمر كذلك بالنسبة للأداء والميزات الإضافية ومجموعة واسعة من البلدان وسهولة الاستخدام.

يحتوي ExpressVPN على كل شيء، مما يجعله خيارنا الأفضل لشبك VPN، حيث تعد ExpressVPN واحدة من أسرع شبكات VPN التي قمنا باختبارها، ولها تطبيق سهل الاستخدام للغاية، جميع خوادمها لا تحتوي على أقراص، وتعمل على تشغيل كل شيء في ذاكرة الوصول العشوائي (RAM) وهي ممارسة مرحب بها أصبحت قياسية إلى حد ما هذه الأيام.

يتمتع ExpressVPN أيضًا بدعم واسع النطاق للأجهزة، بالإضافة إلى ميزة DNS الذكية لأجهزة فك التشفير ووحدات التحكم والمزيد.

إنها ليست أرخص شبكة VPN موجودة، ولكنك تحصل على قيمة قوية مقابل السعر، وتقوم الخدمة بانتظام بجلب مدققين خارجيين لتعزيز بيانات اعتماد الخصوصية الخاصة بها.

NordVPN

الأفضل من حيث الميزات

توصية IMCC: جيد جداً



الإيجابيات	السلبيات
مجموعة ميزات رائعة	أغلى من العديد من المنافسين
سرعات ممتازة	
واجهة جذابة وبديهية	

تمامًا مثل اختيارنا الأفضل يعد NordVPN أيضًا خيارًا ممتازًا. يمكن القول إن Nord مليئة بالميزات أكثر من ExpressVPN، والخدمة ليست سوى جزء واحد من مجموعة أكبر من المنتجات التي تركز على الخصوصية والأمان.

تطبيق سطح المكتب سهل الاستخدام للغاية ويوفر الكثير من الميزات المختلفة بما في ذلك الوصول إلى شبكة TOR عبر VPN ، وشبكات VPN متعددة القفزات، و Meshnet، ومجموعة أمان كاملة مع حظر الإعلانات والبرامج الضارة.

لقد قطعت NordVPN أيضًا شوطًا طويلًا لتعزيز ثقة المستخدم من خلال سياسة عدم الاحتفاظ بالسجلات التي تم التحقق منها بشكل مستقل ثلاث مرات وزيادة شفافية الشركة في السنوات الأخيرة.

تقوم الخدمة أيضًا بإجراء تقييمات البائعين وتستخدم خوادم بدون أقراص لزيادة الأمان.

كما أن سرعاتها رائعة أيضًا، حيث وصلت في المتوسط إلى 73 بالمائة من سرعة الإنترنت الأساسية في اختبارنا عبر جميع الخوادم.

السبب الوحيد الذي جعلنا نضعهم في المرتبة الثانية هو سعر الخدمة، وهو أغلى من ExpressVPN لمجموعة ميزات مماثلة.

ومع ذلك، لا يمكن أن تخطئ إذا قررت استخدام NordVPN باعتباره VPN المفضل لديك.

Mullvad

الأفضل من حيث الخصوصية

توصية IMCC: ممتاز



السلبيات	الإيجابيات
غير مضمون للعمل مع جميع تطبيقات التلفاز	سرعات جيدة
يفتقر إلى الخدمات الإضافية التي تقدمها بعض شبكات VPN	مستوى أعلى من إخفاء الهوية مقارنة بمعظم خدمات VPN
لا توجد حماية بكلمة مرور لحسابك **(هذه ميزة أمان من حيث الخصوصية لأنه لا يطلب التسجيل بعنوان بريدي أو رقم هاتف)**	سطح مكتب Windows سهل الاستخدام

مثلما يهتم Hotspot Shield بالسرعات، فإن Mullvad يهتم بالخصوصية وعدم الكشف عن الهوية.

لم نشهد مطلقًا شبكة VPN أخرى تقاوم بشدة معرفة هويتك بالطريقة التي يفعلها Mullvad

لا يطلب Mullvad عنوان بريدك الإلكتروني أو اسمك أو أي شيء آخر. وبدلاً من ذلك، يقوم بتعيين رقم حساب عشوائي يعمل بمثابة المعرف الخاص بك وتسجيل الدخول.

يقبل Mullvad الدفع باستخدام الطرق التقليدية مثل بطاقات الائتمان وPayPal، ولكن يمكنك أيضًا إرسال دفعتك نقدًا بالبريد لتظل هويتك مخفية قدر الإمكان.

لدى Mullvad سياسة عدم تسجيل الدخول ولا تجمع أي بيانات تعريفية محددة من استخدامك.

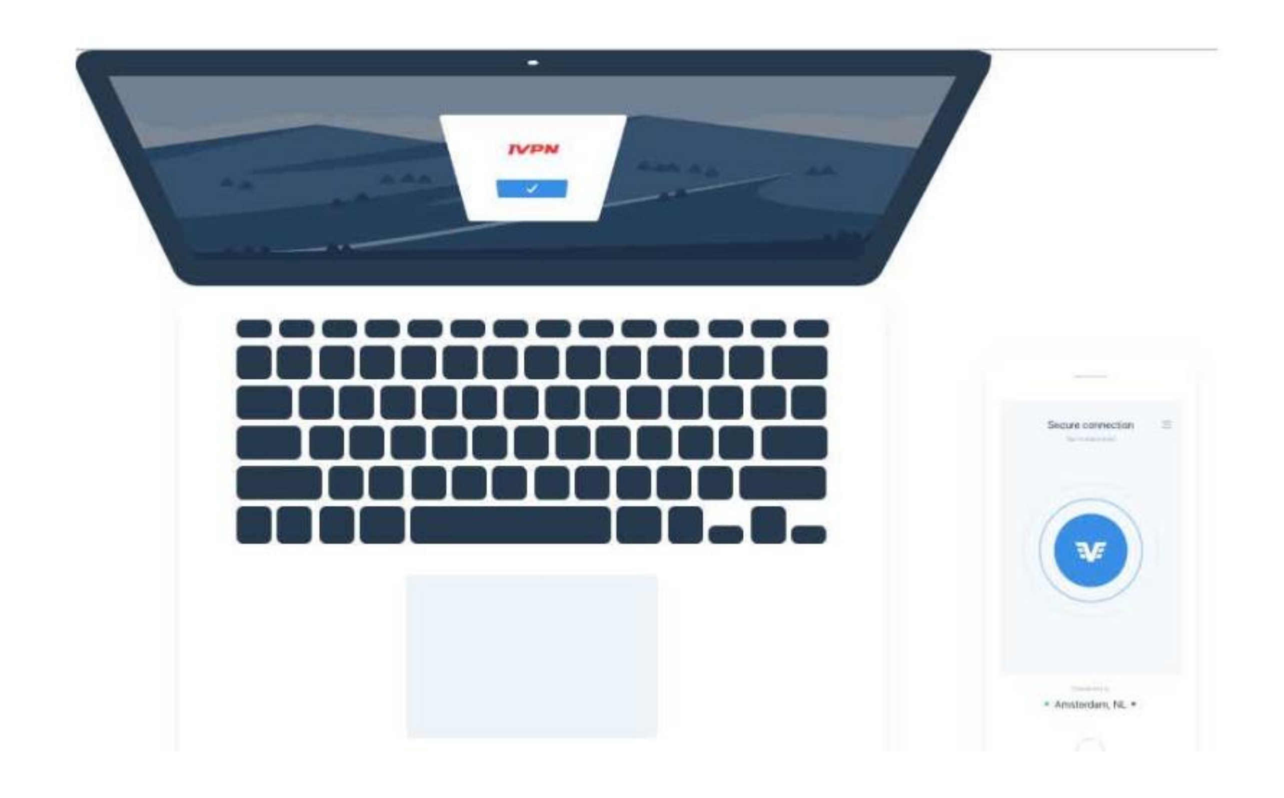
Mullvad يعتبر سريع أيضًا، حيث تم تصنيفه ضمن أفضل خمس سرعات لدينا على الرغم من أننا وجدنا ذلك بشكل غريب على نظام التشغيل Windows.

إلا أن تكوين Mullvad's OpenVPN كان في الواقع أسرع من تكوين Wireguard

IVPN

ثاني افضل VPN من حيث الخصوصية

توصية IMCC: ممتاز



السلبيات	الإيجابيات
إنه على الجانب المكلف بسعر 100 دولار في السنة	سرعات ممتازة لخوادمها في الولايات المتحدة والمملكة المتحدة وأوروبا
شبكة الخوادم أقل من 100 خادم	الواجهة سهلة الفهم
	يتصل بروتوكول WireGuard الافتراضي بسرعة

يأتي IVPN بعد Mullvad من حيث الخصوصية.

انتقلت شبكة VPN التي تتخذ من جبل طارق مقراً لها مؤخرًا إلى التخلص من المعرفات المستندة إلى البريد الإلكتروني والذهاب باستخدام أرقام الحسابات المخصصة عشوائيًا بدلاً من ذلك.

على غرار Mullvad ، فإنه يقبل مجموعة متنوعة من خيارات الدفع للخصوصية بما في ذلك النقد، بالإضافة إلى بطاقات الائتمان التقليدية وPayPal وخيارات أخرى مثل Bitcoin و Monero

لا تُصنف IVPN كواحدة من أسرع شبكات VPN لدينا، ولكنها تتمتع بسرعات مقبولة لمعظم الاستخدامات غير الرسمية.

خيار آخر هو OVPN

لا تصل شبكة VPN هذه إلى المستويات التي تصل إليها Mullvad وIVPN

ولكنها تتطلب فقط اسم مستخدم وكلمة مرور لإنشاء حساب.

لا يتطلب OVPN عنوان بريد إلكتروني، على الرغم من أنه يمكنك إضافة عنوان كدعم لاستعادة الحساب في حالة نسيان كلمة المرور الخاصة بك.

لا يتم تصنيف OVPN ضمن أفضل 10 شبكات لدينا من حيث السرعات، ولكنها تقع خارج قائمة أفضل الشركات أداءً في المرتبة 12.

Hotspot Shield

الأفضل من ناحية السرعة

توصية IMCC: غير موصى به (يحتفظ ببعض سجلات البيانات)



الإيجابيات	السلبيات
سريع جدا	يتم تسجيل زيارات النطاق، على الرغم من عدم ربطها بك **(عيب خطير للغاية من نواحي الخصوصية)**
مجموعة كبيرة من الدول والعديد من الخوادم	غالي الثمن
يتصل بروتوكول WireGuard الافتراضي بسرعة	

في حين أن اختيارنا لأفضل VPN بشكل عام ExpressVPN يتميز بسرعات أعلى من المتوسط، فإن Hotspot Shield على مستوى آخر.

لا توجد خدمة أخرى تقترب من الوصول إلى السرعات التي رأيناها مع هذه الخدمة وهذا ليس مجرد حدث لمرة واحدة أيضًا؛ لقد كان Hotspot Shield دائمًا في المقدمة بسرعات تتراوح بين 12 إلى 15 نقطة مئوية أعلى من المنافسة.

في اختباراتنا حافظ برنامج Hotspot Shield على حوالي 67 بالمائة من السرعة الأساسية. وهذا أسرع بكثير مما ستراه مع معظم خدمات VPN على الرغم من أن تجربتك قد تختلف.

على الجانب السلبي، لا يتيح Hotspot Shield طريقة للدفع بشكل مجهول وقد لا تناسب سياسة الخصوصية الخاصة بالبعض.

ومع ذلك يتمتع Hotspot Shield بسرعات ممتازة، وتطبيقه المكتبي رائع جدًا، وكذلك فهو يعمل مع تطبيقات التلفاز الأمريكي.

Private Internet Access

أفضل VPN لتقسيم الأنفاق split-tunneling

توصية IMCC: ممتاز



السلبيات	الإيجابيات
توجد لوحة التطبيقات بشكل غير مناسب في الركن الأيمن السفلي من الشاشة	تم التحقق بشكل مستقل من سياسة عدم الاحتفاظ بالسجلات
السرعات بالكاد مناسبة	عدد لا يصدق من الخوادم
	ميزات إضافية رائعة مثل القفزات المتعددة والنفق المقسم split-tunneling

إن تطبيق Private Internet Access (PIA) موجودًا منذ فترة وأثبت أنه قادر على الاستمرار في الابتكار والتحسين مع مرور كل عام.

أحدث إصدار من PIA لا يختلف. من خلال تحديث خدمتهم لتشمل اتصالات متزامنة غير محدودة للأجهزة، فقد تم تحسين شبكة VPN القوية بالفعل.

لكن الميزة الحقيقية التي تبرز مع PIA هي ميزة تقسيم الأنفاق، في حين أن هذه ميزة شائعة في معظم الخدمات في هذه القائمة، إلا أن PIA تذهب إلى أبعد من ذلك. فهو لا يسمح للمستخدمين باختيار التطبيقات التي يرغبون في تشغيلها عبر VPN فحسب، بل يسمح لهم أيضًا بتعيين عناوين IP وطلبات DNS أيضًا، حتى أنه يأتي مزودًا بخيار مفتاح الإيقاف القائم على التطبيق، والذي سيحظر حركة المرور على تطبيقات معينة فقط في حالة انقطاع اتصال VPN.

هناك بعض المشكلات الصعبة في الواجهة، كما أن PIA ليست الخدمة الأسرع التي اختبرناها على الإطلاق.

لكن أياً من هذه المشكلات لا يجعل الخدمة أقل قابلية للتطبيق، سيحب المستخدمون المتميزون بشكل خاص جميع التعديلات التي يتيح لك هذا التطبيق القيام بها باستخدام ميزاته الإضافية.

AirVPN

أفضل VPN للتورنت

توصية IMCC: غير موصى به نهائياً (فريق عمل مجهول)



الإيجابيات	السلبيات
سرعات ممتازة	الفريق مجهول إلى حد كبير **(عيب أمني خطير جداً للغاية، ففريق العمل المشغل للتطبيق مجهول بالكامل)**
معلومات مفصلة في الوقت الحقيقي حول الشبكة	
أسعار جيدة مع العديد من خيارات الاشتراك	

تحظى التورنت بسمعة سيئة، وإذا كنا صادقين، فهذا لسبب وجيه، يعد استخدام التورنت هو الطريقة الأولى لتنزيل المواد المقرصنة بما في ذلك الأفلام والبرامج التلفزيونية والموسيقى والألعاب، لكن هذا ليس كل ما يتعلق بالتورنت، إنها طريقة فعالة جدًا لتنزيل البرامج الشرعية مثل توزيعات Linux والمحتوى المعتمد من مواقع مثل BitTorrent Now.

مهما كانت أسبابك، عندما يتعلق الأمر بالتورنت، فإن شبكة VPN تجعل الأمر أسهل، خاصة إذا كانت الشبكة التي تستخدمها تحظر التورنت.

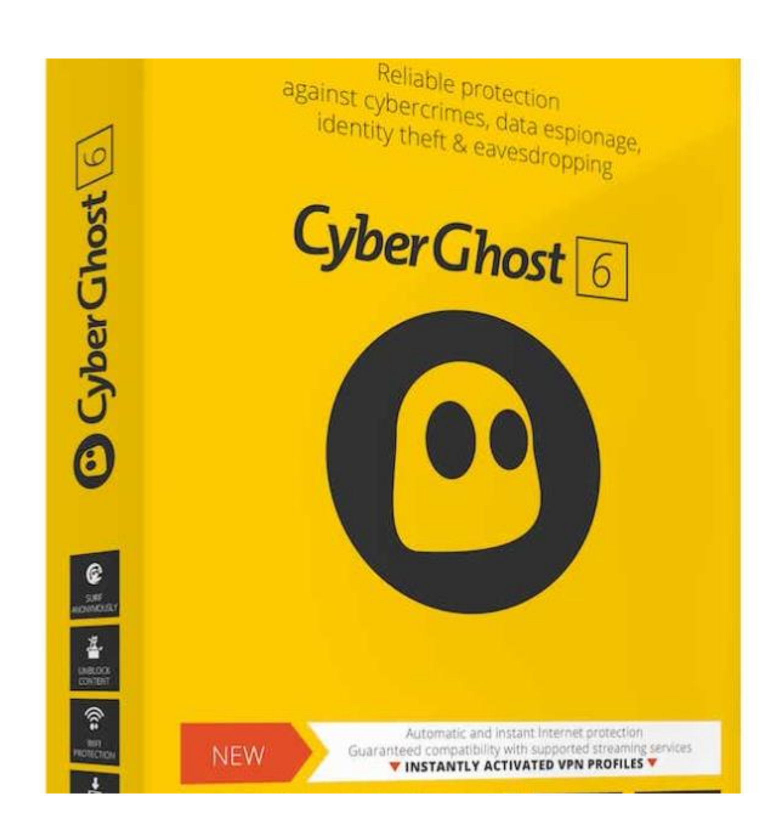
هناك العديد من شبكات VPN من بين أفضل اختياراتنا التي يمكن استخدامها لتنزيل ملفات التورنت، ولكن خيارنا المفضل هوAirVPN .

تتمتع شبكة VPN الخالية من الرتوش بعدد معقول من الخوادم ومواقع الدول، وسرعات جيدة حقًا، وشفافية ممتازة للشبكة، وتركيز على حماية المستخدم، السعر مناسب أيضًا بحوالي 58 دولارًا سنويًا.

CyberGhost VPN

أفضل VPN لمواقع الخوادم

توصية IMCC: متوسط



الإيجابيات	السلبيات
واجهة سهلة الاستخدام	يفتقر إلى بعض الميزات الشائعة مثل القفزات المتعددة وال VPN المزدوج
تم التحقق بشكل مستقل من سياسة عدم تسجيل الدخول	إن سرعات الخادم تكون متفاوتة، خاصة في آسيا
انتشار الخادم مثير للإعجاب بشكل كبير	

إذا كنت تريد التنوع والخيارات في مواقع الخوادم من VPN الخاص بك، فلا يوجد أفضل من CyberGhost VPN إنه يوفر أكثر من 9000 خادم مذهل للمستخدمين للاتصال به، وهو أكثر من ضعف عدد خوادم ExpressVPN على عكس بعض المنافسين.

لا تتركز هذه الخوادم كلها في الولايات المتحدة أو أوروبا أيضًا.

تنتشر خوادمهم في 110 دولة في جميع أنحاء العالم، توصي الخدمة أيضًا بخوادم مُحسّنة للمستخدمين لتلبية الاحتياجات المختلفة مثل الألعاب والبث والتورنت.

في اختباراتنا، وجدنا أن بعض الخوادم كانت أسرع من غيرها، حيث تتمتع الخوادم الموجودة في أوروبا بسرعات ممتازة والخوادم في آسيا ليست جيدة أيضًا.

لكن بشكل عام، تعد السرعات جيدة بما يكفي للقيام بمعظم ما تريد القيام به باستخدام VPN، مثل تصفح الويب والبث وما إلى ذلك.

يحتوي CyberGhost أيضًا على تطبيق Windows مصمم جيدًا وهو بديهي وسهل الاستخدام، حتى عند تعديل إعداداتك.

إنه يفتقر إلى بعض ميزات المستخدم القوية التي توفرها شبكات VPN الأخرى في هذه القائمة، ولكن لا ينبغي أن يكون ذلك بمثابة مشكلة بالنسبة للمستخدم العادي.

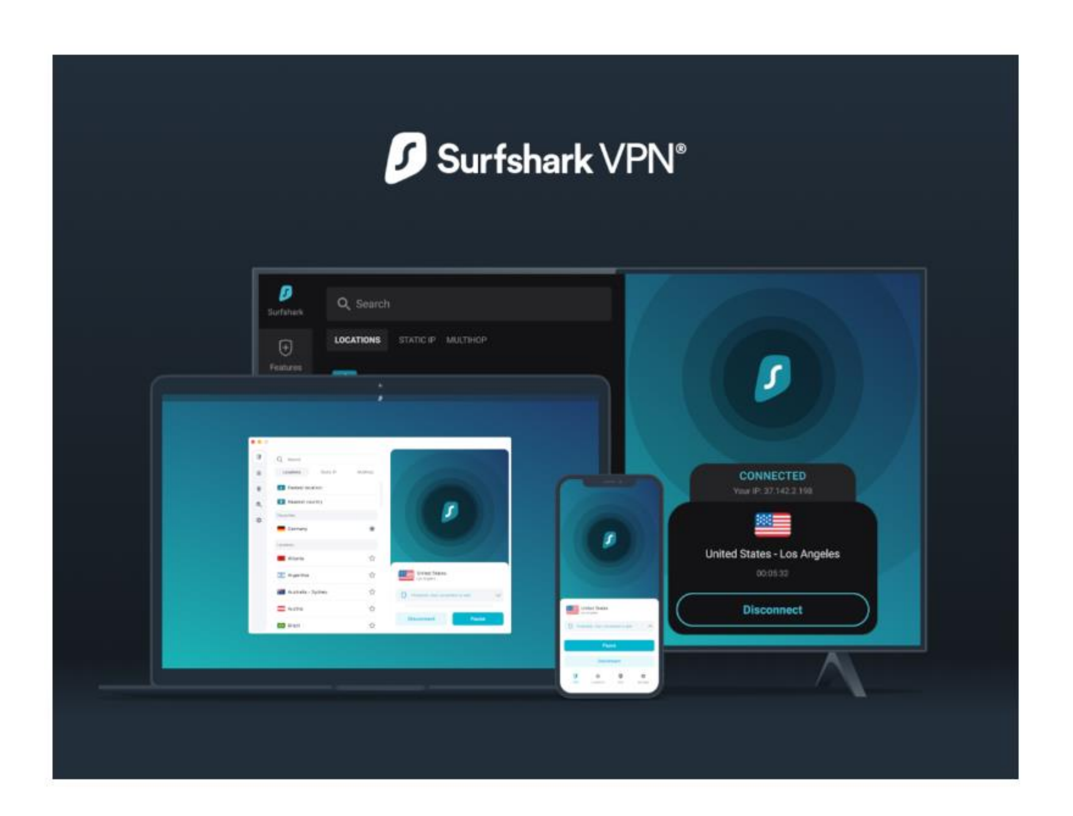
في النهاية، تعد CyberGhost خدمة VPN واضحة وسهلة الاستخدام مع عدد لا يصدق من مواقع الخوادم.

بالنسبة لأولئك الذين يسافرون كثيرًا أو يحتاجون فقط إلى الوصول إلى مجموعة متنوعة وواسعة من الخوادم، فإن CyberGhost يستحق الاختيار بالتأكيد.

Surfshark VPN

أفضل VPN للقفزات المتعددة

توصية IMCC: غير موصى به نهائياً (يخضع لقوانين مشاركة البيانات مع الجهات الحكومية)



الإيجابيات	السلبيات
اتصالات جهاز متزامنة غير محدودة	الإضافات المضمنة مثل تعقب الإعلانات وحظر البرامج الضارة
يعمل بشكل جيد مع جميع تطبيقات التلفاز	لا تتوفر مؤشرات ping أو تحميل الخادم بسهولة
سعر منخفض على الخطط طويلة المدى	يقع مقرها في هولندا وتخضع لطلبات مشاركة البيانات الحكومية **(عيب أمني خطير للغاية، جميع البيانات تخضع للمشاركة مع الحكومة)**

سيحب المستخدمون المتميزون والمهتمون بتحسين إخفاء الهوية وظيفة Surfshark VPN الفريدة متعددة المراحل.

بالنسبة لأولئك الذين قد لا يكونون على دراية بالقفزات المتعددة فهي تسمح لك بتوجيه حركة المرور الخاصة بك من خلال أكثر من خادم خارجي (أي الاتصال بخادم في اليابان، ولكن القفزات المتعددة عبر سنغافورة)، وهذا يزيد من صعوبة تتبع أنشطتك عبر الإنترنت ويزيد من تشويش موقعك الفعلي.

في حين أن العديد من شبكات VPN تقدم الآن ميزة القفزات المتعددة، إلا أن Surfshark يتميز بالسماح للمستخدمين إما باختيار مسار محدد مسبقًا أو إنشاء مسار متعدد القفزات خاص بهم.

علاوة على ذلك، تعمل Surfshark على تنفيذ شبكة Nexus VPN الخاصة بها والتي ستستخدم ميزة Dynamic Multi-Hop لتوصيلك تلقائيًا بأسرع خوادم الدخول والخروج المتوفرة في أي موقع مرغوب، من المفترض أن يؤدي ذلك إلى تحسين سرعات الاتصال في جميع المجالات، لذلك لا يمتلك Surfshark بالفعل واحدة من أفضل ميزات القفزات المتعددة فحسب، بل من المقرر أيضًا أن يتحسن بسرعة فائقة في المستقبل القريب.

AVG Secure

أفضل VPN للمبتدئين

توصية IMCC: غير موصى به (يحتفظ ببعض سجلات للبيانات)



الإيجابيات	السلبيات
سرعات جيدة	يقوم بتسجيل بعض البيانات **(عيب خطير يتعلق بالخصوصية)**
يسمح بـ 10 اتصالات متزامنة ممتازة	لا توجد إمكانية تخصيص حقيقية لمستخدمي الطاقة
سعر منخفض على الخطط طويلة المدى	

إذا كنت تريد شيئًا يتعلق بسهولة الاستخدام فإن AVG Secure هو خيار جيد.

أولاً، أنها تأتي من شركة أمنية معروفة وموثوقة لذلك هناك مخاوف أقل بشأن أمان البيانات مقارنة بإحدى الخدمات المستقلة.

الشيء الرئيسي في AVG Secure هو أن الواجهة سهلة الفهم والاستخدام.

يحتوي على زر "تغيير الموقع" كبير لمساعدتك في تحديد البلد الذي ترغب في الظهور فيه.

ويخبرك التطبيق أيضًا بعنوان IP الحالي الخاص بك ومدة اتصالك بشبك VPN.

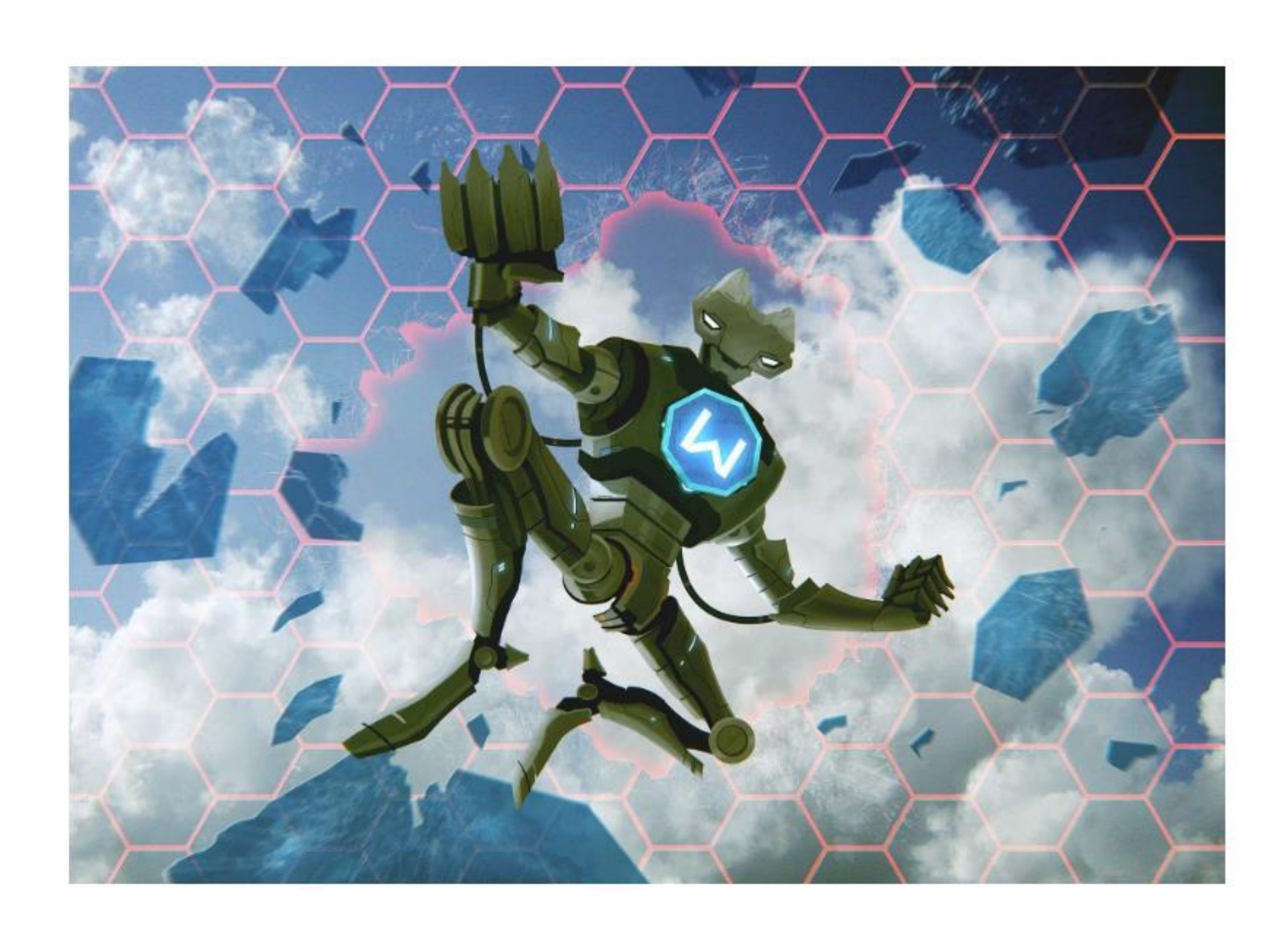
تعمل شبكة VPN هذه أيضًا مع خدمات البث ولديها خوادمP2P .

الشيء الوحيد الذي لا يحتوي عليه هو الكثير من الميزات الإضافية، وهو في الواقع مثالي لأي شخص يبحث عن شبكة VPN خالية من الرتوش.

Windscribe Pro

أفضل VPN للأشخاص ذوي الميزانية المحدودة

توصية IMCC: غير موصى به (سجل أمني مقلق)



السلبيات	الإيجابيات
سجل أمني مقلق مع حادثة الخادم لعام 2021 **(عيب خطير يتعلق بالخصوصية)**	إعداده بسيط
بطء تحميل ملحق المتصفح	أداء جيد
	خطة مجانية رائعة

غالبًا ما يكون اختيار أفضل VPN بالنسبة لك أمرًا مكلفًا. تعد Windscribe Pro واحدة من أرخص الخدمات المتميزة بحوالي 5 دولارات شهريًا (عند الاشتراك سنويًا).

كما أنه سهل الاستخدام حقًا ويوفر أمانًا رائعًا، مع كل من عميل Windows وملحق المتصفح اللذين يعملان جنبًا إلى جنب للحفاظ على خصوصية التصفح وخاليًا من النوافذ المنبثقة.

يتيح لك Windscribe أيضًا انتقاء واختيار الميزات التي تريدها عبر نظام بناء الخطة الذي يسمح بتنوع كبير لتلبية احتياجات كل مستخدم.

يعد خيار Windscribe المجاني في حد ذاته خيارًا جيدًا للاستخدام، وهو اختبار جيد قبل اتخاذ قرار بشأن النسخة المدفوعة.

PersonalVPN

أفضل شبكة VPN مقرها الولايات المتحدة

غير موصى به (سجل أمني مقلق)



الإيجابيات	السلبيات
سعره معقول	ليس هناك الكثير من الميزات الإضافية أو المتخصصة
خوادم سريعة في العديد من المواقع حول العالم	يحتوي التسعير المتدرج على خيارات غريبة للميزات العالية
جيد لمستخدمي الطاقة والمبتدئين	

إذا كنت تريد شبكة VPN مقرها في الولايات المتحدة الأمريكية، فإننا نوصي باستخدام PersonalVPN من WiTopia .

السرعات جيدة، والسعر مناسب، والتطبيق سهل الاستخدام للغاية.

صحيح أن الكثير من مواقع مراجعة VPN تؤكد على أهمية وجود شبكة VPN خارج ما يسمى بدول العيون الخمس والتي تشمل الولايات المتحدة، حتى أن البعض سيقول لتجنب العيون الأربعة عشر، الفكرة هي أنه إذا كنت تستخدم شبكة VPN مقرها الولايات المتحدة فقد ينتهي الأمر بمراقبة أنشطتك سرًا من قبل السلطات.

كشف سنودن عن مثل هذه الحقائق في عام 2013.

ولكن إذا كنت تستخدم VPN للوصول إلى حساباتك على Gmail أو Facebook أو Twitter أو Instagram أو أي خدمة أخرى مقرها الولايات المتحدة، فإن البقاء خارج العيون الأربعة عشر لا معنى له إلى حد ما.

من المؤكد أن شبكة VPN ذات اللغة الغريبة (الغير انجليزية) قد تكون قادرة على تجاهل مذكرات الاستدعاء الأمريكية بسهولة للحصول على البيانات، ولكن الخدمات الأمريكية عبر الإنترنت التي تستخدمها هي قصة أخرى.

علاوة على ذلك، إذا أخطأت شبكة VPN أمريكية في حقك، فسيكون محاسبتها أسهل كثيرًا من تلك الموجودة في سنغافورة، أو حتى السويد.

ما هو ال VPN

تقوم شبكات VPN بإنشاء نفق آمن بين جهاز الكمبيوتر الخاص بك والإنترنت. يمكنك الاتصال بخادمVPN ، والذي يمكن أن يكون موجودًا في الولايات المتحدة أو في دولة أجنبية، مثل فرنسا أو اليابان. تمر حركة مرور الويب الخاصة بك بعد ذلك عبر هذا الخادم لتظهر كما لو كنت تتصفح من موقع ذلك الخادم، وليس من موقعك الفعلي.

عندما تستخدمVPN ، يصعب على الآخرين التطفل على نشاط تصفح الويب الخاص بك. أنت فقط وخدمة VPN والموقع الإلكتروني الذي تزوره ستعرف ما تنوي فعله.

يمكن أن تكون شبكة VPN استجابة رائعة لمجموعة متنوعة من المخاوف، مثل الخصوصية عبر الإنترنت، وعدم الكشف عن هويتك، وزيادة الأمان على شبكة Wi-Fi العامة، وبالطبع انتحال المواقع.

في حين أن شبكة VPN يمكن أن تساعد في الحفاظ على الخصوصية وإخفاء الهوية، إلا أنني لا أوصي بإثارة الثورة السياسية العظيمة القادمة من خلال الاعتماد فقط على شبكة .VPN لكي تصبح شبحًا على الإنترنت (أو أقرب ما يمكنك الوصول إليه بشكل واقعي)، فإن الأمر يتطلب أكثر بكثير من اشتراك شهري بقيمة 5 دولارات في.VPN

علاوة على ذلك، تعد شبكة VPN خيارًا ممتازًا للبقاء آمنًا أثناء استخدام شبكة Wi-Fi في المطار أو المقهى المحلي لديك. يمكن للمتسللين الذين يستخدمون شبكة Wi-Fi عامة محاولة اختراق جهاز الكمبيوتر الخاص بك، لكن شبكة VPN تجعل هذه المهمة أكثر صعوبة.

أخيرًا، قد ترغب في أن تقوم شبكة VPN بانتحال موقعك لتنزيل المحتوى الذي لا ينبغي لك الوصول إليه، ولكن هذا أيضًا له حدود. اعتادت شبكة VPN أن تكون الحل الأمثل

لمشاهدة البرامج المقصر مشاهدتها على دولة معينة، وفي محاولات الشركات لمنع هذا التحايل عملت على محاولات حثيثة لاكتشاف مستخدمي ال VPN وحظرهم من استخدام منتجاتها، ورغم ذلك فإن هذه المهمة صعبة للغاية.

ملاحظة أخيرة للتحذير: لا تعتمد على VPN الخاص بك لحماية المعلومات المصرفية على اتصال Wi-Fi مفتوح. كلما كان ذلك ممكنًا، اترك التعاملات المالية عبر الإنترنت للمنزل عبر اتصال سلكي قوي.

ما الذي تبحث عنه في ال VPN

قبل أي شيء آخر، عليك أن تفهم أنه إذا كنت تريد استخدام VPN فيجب أن تدفع مقابل ذلك.

تبيع شبكات VPN المجانية عادةً بيانات التصفح الخاصة بك في شكل مجمع للباحثين والمسوقين، أو تمنحك قدرًا ضئيلًا من نقل البيانات كل شهر. وفي كلتا الحالتين، القاعدة الأساسية هي أن شبكة VPN المجانية لن تحمي خصوصيتك بأي طريقة مجدية.

الشيء التالي الذي يجب مراعاته هو سياسات التسجيل الخاصة بشبكة VPN ، بمعنى آخر ما نوع البيانات التي تجمعها الخدمة عنك وعن نشاط VPN الخاص بك وما هي مدة حفظ هذه البيانات؟

الخصوصية هي المبدأ الأساسي لشبكة VPN، وما الفائدة من تجنب المراقبة الحكومية السلبية فقط لكي يقوم مزود VPN بتسجيل جميع زيارات موقع الويب الخاص بك؟

من الناحية المثالية، ستقول شبكة VPN إنها تحتفظ فقط بالسجلات لفترات قصيرة.

على سبيل المثال، يقوم بعض مقدمي الخدمات بتسجيل النشاط في ذاكرة الوصول العشوائي (RAM) فقط أثناء الجلسة أو يرسلون جميع السجلات تلقائيًا إلى النسيان بمجرد إنشائها. قد يحتفظ مقدمو الخدمة الآخرون بالسجلات لبضع ساعات أو أيام أو أسابيع أو حتى أشهر.

تختلف سياسات VPN أيضًا عندما يتعلق الأمر بالمعلومات الشخصية، تريد بعض شبكات VPN معرفة القليل جدًا عنك، وتفضل أن يقوم المستخدمون بتسجيل الدخول باستخدام اسم مستعار والدفع باستخدام البيتكوين، يعد هذا أمرًا غريبًا بعض الشيء بالنسبة لمعظم الناس، ولهذا السبب تقبل العديد من الخدمات أيضًا PayPal.

الدفع بهذه الطريقة ليس مثاليًا للخصوصية، ولكنه يعني أن الشبكة الافتراضية الخاصة لا تحتفظ بمعلومات الدفع الخاصة بك - على الرغم من أنها ستكون متاحة من خلال PayPal.

بعد سياسات التسجيل، تريد معرفة عدد الخوادم التي تقدمها VPN وعدد اتصالات الدولة التي لديها، يوفر عدد الخوادم فكرة عن مقدار التحميل الذي يمكن أن تتحمله شبكة VPN قبل أن تتباطأ إلى الزحف بسبب حركة المرور الهائلة.

وفي الوقت نفسه، فإن اتصالات الدول هي الأكثر أهمية بالنسبة لأولئك الذين يريدون محاكاة مواقعهم؛ ومع ذلك يجب على غير المخادعين أيضًا التأكد من وجود اتصالات في بلدهم الأصلي.

إذا كنت تعيش في لوس أنجلوس، على سبيل المثال، وتريد الوصول إلى المحتوى الأمريكي، فستحتاج إلى شبكة VPN توفر اتصالات أمريكية فلن تنجح تجربة مشاهدة Amazon Prime Video عبر اتصال VPN هولندي، لأنه بقدر ما يتعلق الأمر بأمازون، سيكون جهاز الكمبيوتر الخاص بك موجودًا في هولندا.

سيرغب بعض المستخدمين أيضًا في البحث عن سياسات مشاركة الملفات من نظير إلى نظير (P2P) الخاصة بموفر VPN هناك شبكات VPN تمنع التورنت، بعض أنواع ال VPN تغظ النضر عن هذا الشي، لكنهم سوف يبيعونك بسرعة إذا كنت تنوي عمل شيئ غير قانوني.

P2P ليس محور اهتمامنا الرئيسي هنا، ولكننا سنلاحظ في كل مراجعة ما إذا كان مزود معين يسمح بمشاركة الملفات أم لا.

وأخيرًا، ما هو عدد الأجهزة التي تدعمها شبكة VPN من حساب واحد؟ في عصر الهواتف الذكية والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية، يجب أن تشمل تكلفة VPN ترخيصًا لخمسة أجهزة على الأقل، بالإضافة إلى ذلك يجب أن يكون لدى

مقدم الخدمة تطبيقات Android و iOS لتسهيل توصيل الهاتف الذكي أو الجهاز اللوحي بالخدمة.

كيف قمنا بالاختبار

نحن نحكم على شبكات VPN بناءً على مجموعة متنوعة من المعايير بما في ذلك سرعات الاتصال الإجمالية وحماية الخصوصية وسهولة استخدام الواجهة واختيارات البلد وعدد الخوادم والتكلفة.

يتم الاحتفاظ باختبارات السرعة بسيطة قدر الإمكان، نحن نتصل بخمسة مواقع عالمية مختلفة لشبكة VPN معينة - عادةً أمريكا الشمالية وأوروبا والمملكة المتحدة وأستراليا وبطاقة شاملة في مكان ما في آسيا - في ثلاثة أيام مختلفة في أوقات مختلفة من اليوم ونجري الاختبار في كل موقع عدة مرات.

قبل أن يبدأ الاختبار، نتحقق من سرعة اتصال Wi-Fi الأساسي لدينا باستخدام اختبار السرعة عبر الإنترنت، ثم نتصل بخوادم VPN حول العالم ونجري اختبار السرعة مرة أخرى. نعرض بعد ذلك كل نتيجة، ونحسب متوسطها، ونحسب المتوسط كنسبة مئوية من السرعة الأساسية.

تذكر أن سرعات الإنترنت يمكن أن تختلف بشكل كبير بناءً على الموقع وأجهزة التوجيه وأجهزة الكمبيوتر والوقت من اليوم ونوع الاتصال والحمل على VPN وخوادم اختبار السرعة والعديد من العوامل الأخرى، بمعنى آخر من المحتمل أن تختلف نتائج اختباراتنا عن نتائجك، لهذا السبب اعتبر نتائج السرعة لدينا بمثابة دليل تقريبي لكيفية أداء كل شبكة VPN.

يتم أيضًا الحفاظ على سهولة الحكم على اختيارات الخادم حسب البلد، نتوقع أن توفر شبكة VPN مجموعة متنوعة من اتصالات البلدان بحد أدنى 20 اتصالاً.

يتم الحكم على الخصوصية وعدم الكشف عن الهوية بناءً على الضمانات التي تقدمها الشركات، بالإضافة إلى سمعتها من خلال أي أخبار نعلم أنها قد تؤثر على مصداقية هذه الادعاءات.

نلقي أيضًا نظرة على تشفير البيانات والمصادقة وبروتوكولات المصافحة المستخدمة.

أخيرًا، بالنسبة للتسعير، نتوقع أن ندفع 60 دولارًا سنويًا، وأي شيء يزيد عن ذلك يحتاج إلى تبرير تكلفته بميزات إضافية أو نقاط بيع فريدة من نوع ما.

شبكات VPN بارزة أخرى

هناك العديد من شبكات VPN الجديرة بالاهتمام أكثر من مجرد المفضلة لدينا المذكورة أعلاه، بما في ذلك

AVG Internet Security, CyberGhost, ESET Security Premium, FastestVPN, Hide.me, HMA Pro 4, OVPN, Trend Micro Maximum Security, Windscribe Pro, Perfect Privacy, PrivateVPN by TrunkSpace Hosting, PureVPN, Speedify 10, VPNCity, ClearVPN, Malwarebytes Privacy, TorGuard, VeePN, AceVPN.com, SurfEasy.

سنستمر في تقييم الخدمات الجديدة وإعادة تقييم الخدمات التي اختبرناها بالفعل بشكل منتظم، لذا تأكد من العودة لمعرفة ما قمنا به أيضًا من خلال عملهم.

الأسئلة المتكررة

هل من القانوني استخدام VPN؟

نعم! من القانوني تمامًا في معظم البلدان بما في ذلك الولايات المتحدة استخدامVPN .

أثناء استخدام VPN قد تجد بعض مواقع الويب التي تحاول حظر اتصالك، ولكن هذه سياسة استخدام خاصة بموقع ويب فردي وليس لها علاقة بشرعية VPN نفسها.

هناك شيء واحد يجب ملاحظته، على الرغم من أنه من القانوني استخدام VPN ، فإن بعض الأنشطة التي تتم أثناء استخدام VPN قد تكون غير قانونية، أشياء مثل تنزيل محتوى مقرصن محمي بحقوق الطبع والنشر أو الوصول إلى أسواق الويب المظلمة تعتبر غير قانونية سواء كنت تستخدم VPN أم لا.

هل تحمي شبكات VPN من البرامج الضارة وفيروسات الكمبيوتر؟

لا، اتصال VPN نفسه لا يحميك من البرامج الضارة وفيروسات الكمبيوتر، ومع ذلك فهو يقوم بتشفير حركة المرور الخاصة بك على الإنترنت ويمنع أعين المتطفلين من الوصول إلى سجل التصفح الخاص بك.

ومع ذلك، توفر بعض خدمات VPN، مثل Nord VPN، ميزات أمان إضافية مثل أدوات حظر الإعلانات والبرامج الضارة.

بالإضافة إلى ذلك تقدم العديد من مجموعات مكافحة الفيروسات الآن خدمات VPN إلى جانب ميزات الأمان الخاصة بها.

على الرغم من استخدام الشبكات الافتراضية الخاصة وبرامج مكافحة الفيروسات لأغراض مختلفة، إلا أنه لا تزال هناك درجة من التداخل تجعل استخدام كلتا الأداتين معًا مفيدًا.

هل ستؤثر شبكة VPN على سرعات الإنترنت الخاصة بي؟

على الأرجح ستلاحظ انخفاضًا معتدلًا في سرعة الإنترنت لديك أثناء استخدام VPN ويرجع ذلك أساسًا إلى عملية إعادة توجيه حركة المرور على الإنترنت وتشفيرها من خلال خادم VPN قبل التوجه إلى وجهتها.

يعتمد مقدار زمن الوصول الذي ستواجهه خلال هذه العملية على خادم البلد الذي تختاره لتوكيل حركة المرور الخاصة بك من خلاله، إذا اخترت خادمًا يقع على الجانب الآخر من العالم فستلاحظ تأثرا أكبر بكثير مما لو كنت تتصل بخادم قريب في نفس بلدك.

ولحسن الحظ، يجب أن تتمتع معظم شبكات VPN الحديثة بالبنية التحتية اللازمة للحفاظ على معدلات نقل بيانات عالية السرعة وآمنة، لذلك من المحتمل أنه لا يزال بإمكانك التصفح والبث دون أي تأثير ملحوظ أثناء استخدام شبكة VPN حسنة السمعة مثل تلك المذكورة أعلاه.

هل ستجعلني شبكة VPN مجهولاً عبر الإنترنت؟

لسوء الحظ الأمر ليس بهذه البساطة مثل تشغيل VPN الخاص بك والاختفاء خارج الشبكة، على الرغم من أن شبكات VPN توفر بالتأكيد خصوصية وأمانًا أفضل، إلا أنها لا تجعلك مجهول الهوية تمامًا.

هناك عدد مذهل من الطرق التي تتبعها الشركات عبر الإنترنت ولا تستطيع شبكة VPN حظرها جميعًا، على سبيل المثال عند تسجيل الدخول إلى موقع ويب يتم الكشف عن هويتك لذلك الموقع أو عند تسجيل الدخول إلى حساب Gmail الخاص بك أثناء استخدام VPN، يمكن لـ Google الآن جمع ملفات تعريف الارتباط بناءً على تصفحك.

توصية IMCC: راجع كتاب الجزء الأول من الحرب الإلكترونية -الأمن السيبراني- من إعداد مجلس التعاون الإعلامي الإسلامي للمزيد حول الإجراءات اللازمة لإخفاء هويتك تماماً عبر الإنترنت.

كم عدد الخوادم التي يجب أن يمتلكها VPN الخاص بي؟

لا يوجد عدد محدد من الخوادم التي تجعل أحد VPN أفضل من الآخر. ومع ذلك، فإن معظم موفري VPN الرئيسيين يقدمون ما بين 3000 إلى 5000 خادم. نوصي أيضًا بتجنب أي خدمات مدفوعة يمتلك مقدموها أقل من 1000 خادم لأن هذا قد يكون مؤشرًا على أن الشركة ليست راسخة بعد، مما يعني أن هناك فرصة أكبر لمشاكل الموثوقية.

من الشائع أن يقوم موفرو VPN بالإعلان عن عدد الخوادم التي لديهم، ولكن هذا يعد وسيلة للتحايل التسويقي إلى حد كبير ولا يعادل بشكل عام جودة مزود VPN نفسه. أشياء مثل انتشار مواقع الخوادم وجودة الخادم لا تقل أهمية، إن لم تكن أكثر، عن عدد الخوادم المتاحة.

ملاحظة المحرر: نظرًا لأن الخدمات عبر الإنترنت غالبًا ما تكون متكررة، وتكتسب ميزات جديدة وتحسينات في الأداء بمرور الوقت، فإن مراجعاتنا تخضع للتغيير لتعكس الحالة الحالية للخدمات بدقة.

مع تحيات إخواكم في جيش الملاحم الإلكتروني

و

مجلس التعاون الإعلامي الإسلامي

تتصح بمراجعة كتاب الحرب الإلكترونية الجزء الأول – الأمن السيبراني –

من إعداد مجلس التعاون الإعلامي الإسلامي

أفضل تطبيق آمن للمراسلة

كيف تختار تطبيق المراسلة الذي تستخدمه؟

إعداد: مجلس التعاون الإعلامي الإسلامي

تقديم: جيش الملاحم الإلكتروني



Al-Malahem Electronic Army

بسم الله الرحمن الرحيم

جيش الملاحم الإلكتروني

يقدم

*** دراسة ملحقة: ما هو أفضل تطبيق آمن للمراسلة ***

كيف تختار تطبيق المراسلة الذي تستخدمه

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

المصدر

https://nordvpn.com/blog/most-secure-messaging-app/

المقدمة

يحافظ تطبيق المراسلة الآمن، مثل WhatsApp، على خصوصية محادثاتك. ولكن كم ماهي دقة هذا الوصف؟! سواء كانت قصة محرجة، أو ثرثرة في المكتب، أو الانفتاح على مشاعرك، فإن آخر شيء تريده هو أن يرى شخص ما رسائلك أو يستخدمها لعرض إعلاناتك. ما لم تكن تستخدم تطبيق مراسلة مشفر، فإنك تترك كل شيء في العلن.

بينما يلعب التشفير والخصوصية دورًا حيويًا في اختيار تطبيق المراسلة الذي سيتم استخدامه، فمن الضروري أيضًا استخدام تطبيقات المراسلة التي يستخدمها أصدقاؤنا.

وفقًا لـ Statista (2022)، تظل WeChat وWhatsApp وFacebook Messenger أكثر تطبيقات المراسلة شيوعًا في العالم على الرغم من ممارسات الخصوصية المشكوك فيها لدى Facebook.

تطبيقات المراسلة الأكثر شعبية حسب البلد

Country	App
Germany	WhatsApp **95%**
China	WeChat **81%**
Spain	WhatsApp **92%**
Italy	WhatsApp **97%**
France	FB Messenger **59%**
Denmark	FB Messenger **72%**
Finland	WhatsApp **95%**
Sweden	FB Messenger **64%**
UK	WhatsApp **71%**
US	FB Messenger **83%**
India	WhatsApp **97%**
Singapore	WhatsApp **83%**
Austria	WhatsApp **94%**
Brazil	WhatsApp **99%**

- يستخدم تطبيق WhatsApp ما يزيد عن 90% من الأشخاص في البلدان التي يعتبر فيها تطبيق المراسلة الرائد. في الواقع، يعد تطبيق WhatsApp هو تطبيق المراسلة الأكثر استخدامًا على مستوى العالم.

- في عام 2022، يستخدم حوالي 83% من الولايات المتحدة تطبيق Facebook Messenger، في حين يختار غالبية سكان أمريكا اللاتينية تطبيق WhatsApp.

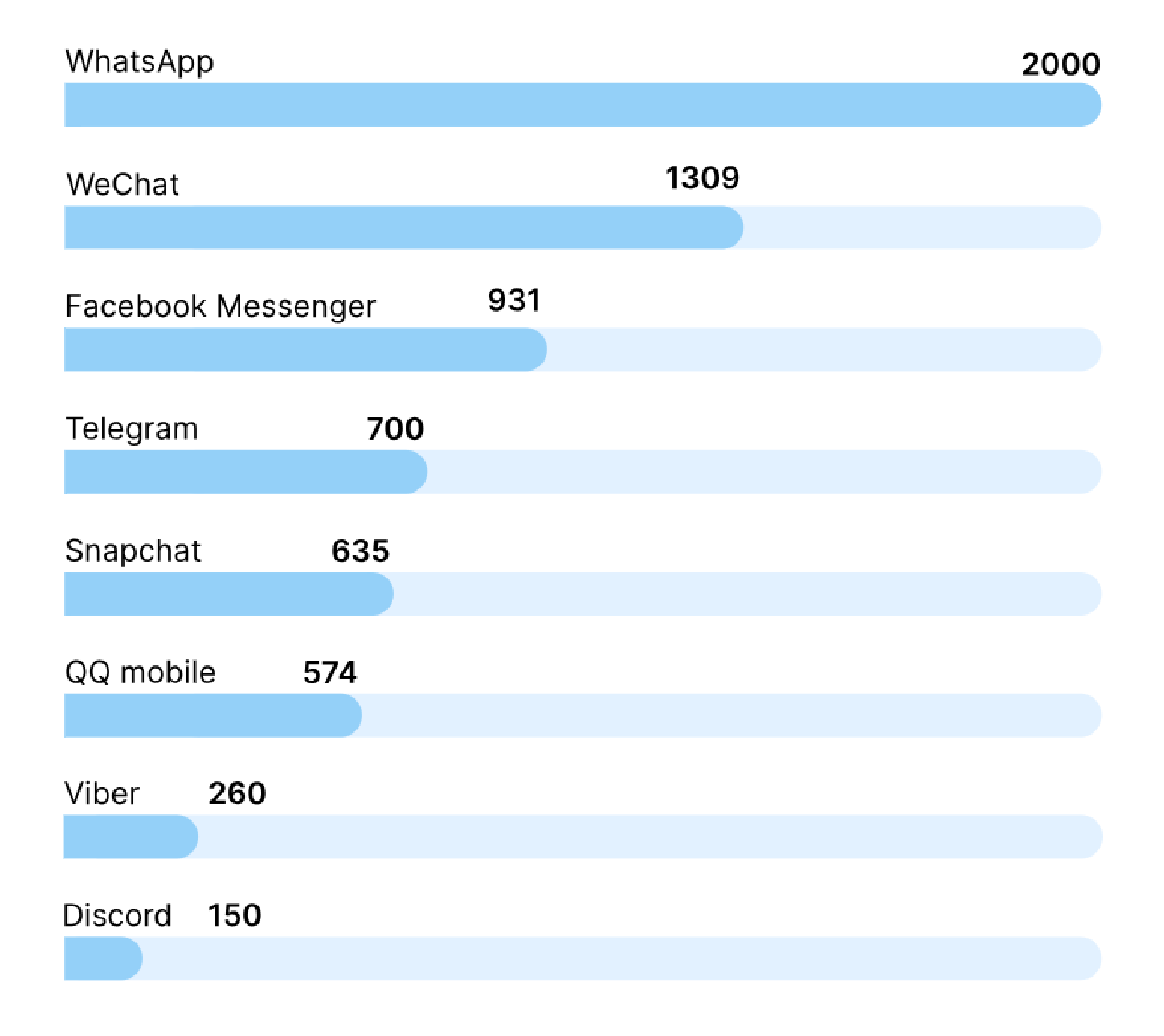
- يمتلك فيسبوك اثنتين من الشركات الرائدة في السوق (WhatsApp و Facebook Messenger)، مما يعني أن معظم العالم يستخدم تطبيقات المراسلة المملوكة لفيسبوك.

- يستخدم WeChat غالبية الأشخاص في الصين، نظرًا لأن تطبيقات مثل WhatsApp وFacebook Messenger محظورة.

- يواجه تطبيق Telegram، المعروف بضوابطه الصارمة على الخصوصية، صعوبة في الحصول على جاذبية جماهيرية، حيث أن معظم مستخدميه يقيمون في الشرق الأوسط.

- أصبح الأمان والخصوصية داخل تطبيقات المراسلة أكثر أهمية. إذا كان الأمان هو نقطة اهتمامك الأولى بدلاً من الشعبية، فتابع القراءة.

أكثر تطبيقات المراسلة شعبية بناءً على عدد المستخدمين النشطين شهريًا (بالملايين)



WhatsApp 2000 , WeChat 1309 , Facebook Messenger 931 , Telegram 700 , Snapchat 635 , QQ mobile 574 , Viber 260 , Discord 150

كيفية اختيار تطبيق المراسلة الآمن

اختر تطبيقًا يستخدم التشفير الشامل والتعليمات البرمجية مفتوحة المصدر ولا يخزن بياناتك.

العديد من تطبيقات المراسلة المتوفرة في السوق ليست كلها آمنة كما يدعون في الواقع، حتى تطبيق المراسلة الأكثر شيوعًا في العالم ليس محصنًا ضد عمليات الاحتيال (راجع عمليات الاحتيال على WhatsApp).

لتسهيل اختيارك، قمنا بتجميع قائمة من التطبيقات التي توفر التشفير الشامل، مما يعني أنه لا يمكن لأحد رؤية محادثاتك ما لم يكن لديه مفتاح خاص لفك تشفير رسالتك.

والأهم من ذلك، أن هذا يعني أنه حتى مقدم الخدمة لا يمكنه رؤية رسائلك - ولا حتى أصحاب العمل المسيئين، أو المتسللين، أو المسؤولين الحكوميين. ومع ذلك، فإن ميزاتها الإضافية وعيوبها كلها مختلفة.

لقد قمنا بمراجعة 10 تطبيقات مراسلة مشفرة وعرضنا إيجابياتها وسلبياتها.

Viber

الإيجابيات	السلبيات
تشفير E2E تشفير كامل بمفاتيح تشفير لا يمكن فكها إلا من قبل المتلقي	يجمع البيانات حول المستخدمين وجهات الاتصال الخاصة بهم **(عيب خطير، ليس الأفضل للخصوصية)**
رسائل التدمير الذاتي	يتتبع نشاط المستخدمين على وسائل التواصل الاجتماعي **(عيب أمني خطير لتتبع المستخدمين)**
دعم واسع للجهاز	

تم تصميم Viber، وهو أحد أقوى منافسي WhatsApp، في البداية لإجراء مكالمات عبر الإنترنت ولكنه سرعان ما تطور ليصبح تطبيق دردشة متكامل.

يمكنك استخدامه لإرسال الرسائل الصوتية والنصية والصور ومقاطع الفيديو إلى مستخدمين ومجموعات من المستخدمين الآخرين. جميع الدردشات، بما في ذلك الدردشات الجماعية، مشفرة بالكامل.

مكنك استخدام Viber على الأجهزة المحمولة ومعظم أنظمة تشغيل سطح المكتب.

ومع ذلك، فإن إحدى ميزات Viber الأكثر جاذبية هي رسائل التدمير الذاتي. ولكن هذا هو المكان الذي تنتهي فيه الأخبار الجيدة..

تشتهر الشركة بجمع الأسماء وأرقام هواتف مستخدميها الفرديين بالإضافة إلى الأشخاص الموجودين في قوائم الاتصال الخاصة بالمستخدمين، حتى لو كان هؤلاء الأشخاص لا يستخدمون فايبر. يذهب Viber إلى حد متابعة نشاط مستخدميه على الشبكات الاجتماعية. فهو يستخدم جميع البيانات الوصفية التي يمكنه الحصول عليها، لذا فإن استخدام خدمات فايبر يعد أمرًا محفوفًا بالمخاطر.

WhatsApp

الإيجابيات	السلبيات
يستخدم تشفير Signal	مملوكة للفيسبوك **(الشركة مشهورة بجمع البيانات ونشاطات المستخدمين وتتبعهم وانتهاك خصوصيتهم)**
من المحتمل أن معظم أصدقائك يستخدمونه	شهدت خرقا كبيرا **(حوادث اختراق سابقة وثغرات أمنية)**
سهل الاستخدام ويوفر ميزات إضافية	

مع أكثر من مليار مستخدم، يعد تطبيق WhatsApp أحد تطبيقات المراسلة الأكثر استخدامًا على نطاق واسع. إنه سهل الاستخدام ويوفر ميزات مثل مشاركة الموقع والملفات والصور المتحركة وحتى دعم سطح المكتب. كما أنه يستخدم بروتوكول التشفير القوي الذي تم تطويره لـ Signal بواسطة Open Whisper Systems، والذي يعتبر معيار الصناعة.

يتميز التشفير بالسرية التامة للأمام (PFS). وهذا يعني أنه إذا تمكن شخص ما من سرقة مفتاح فك التشفير لمحادثتك، فلن يتمكن إلا من رؤية الرسالة الأخيرة التي أرسلتها. كل شيء آخر سيبقى خاصا..

ومن ناحية أخرى، فإن تطبيق WhatsApp مملوك لشركة Facebook، مما يثير مخاوف أمنية كبيرة. يقع جمع بيانات المستخدمين في قلب نموذج أعمال عملاق التواصل الاجتماعي، وقد فشل في الحفاظ على أمان بيانات المستخدم عدة مرات. هل يمكننا حقًا أن نثق بفيسبوك، على الرغم من التشفير الآمن؟

في 14 مايو 2019، اكتشف المتسللون ثغرة أمنية خطيرة في تطبيق WhatsApp واستخدموها لتثبيت برامج ضارة للمراقبة على عدد محدد من الهواتف. تم إدخال برنامج التجسس هذا من خلال مكالمات WhatsApp الصوتية (لم يكن الشخص المستهدف بحاجة إلى الرد على المكالمة) ومنح المتسللين إمكانية الوصول إلى الرسائل النصية للضحايا، ورسائل البريد الإلكتروني، ورسائل WhatsApp، وتفاصيل الاتصال، وسجلات المكالمات، والموقع، والميكروفون، والكاميرا. لقد تم الآن تصحيح الثغرة الأمنية.

(الدراسة هنا تقصد برنامج بيجاسوس الإسرائيلي)

Facebook Messenger

الإيجابيات	السلبيات
ربما يستخدمه معظم أصدقائك	التشفير ليس افتراضيًا **(يجب عليك تفعيل خيار التشفير يدوياً والذي قد يكون بحد ذاته عملية فرز بيانات لمعرفة من مهتم بالتشفير عن البقية)**
يمكنك استخدامه حتى لو قمت بإلغاء تنشيط حسابك على Facebook	لا يقوم بتشفير المحادثات السابقة
	يتتبع سلوكك **(خطر كبير في انتهاك الخصوصية)**

يستخدم مليارات الأشخاص فيسبوك وخدمات المراسلة الخاصة به، لكن القليل منهم يعلم أن تطبيق الشركة يوفر ميزة التشفير التام بين الطرفين. وذلك لأن Facebook قام بعمل رائع في إخفاء هذه الميزة. (تعرف على كيفية بدء محادثة سرية على Facebook هنا)
https://nordvpn.com/blog/facebook-secret-conversation/

من المثير للإعجاب أن فيسبوك قدم هذه الميزة، لكن هذا لا يغير حقيقة أن عملاق الوسائط الاجتماعية يجمع بيانات مثل من تراسله أو عدد مرات استخدامك للتطبيق. ودعونا لا ننسى أنه في عام 2018، أصبح فيسبوك مشهورًا بسبب خروقاته المتعددة للبيانات. أصبح من الصعب الوثوق بخصوصية محادثاتك.!

iMessage

الإيجابيات	السلبيات
يتشغل التشفير بشكل افتراضي	جمع معلومات المستخدم بناءً على سلوكهم **(عيب خطير في انتهاك الخصوصية)**
برنامج سطح مكتب سهل الاستخدام	فشل في تشفير البيانات الحساسة الأخرى مثل أرقام الهواتف المحمولة أو البيانات الوصفية أو البيانات المخزنة في السحاب
دعم واسع للجهاز	

ليس هناك شك في أن منتجات Apple تتمتع بسمعة جيدة عندما يتعلق الأمر بالأمن السيبراني. البديل الذي يستخدمه أصحاب iPhone للرسائل النصية – iMessage – لديه تشفير افتراضي بين الطرفين. ومع ذلك، فإنه لا يزال يحتوي على العديد من نقاط الضعف وهو بعيد عن منصة المراسلة الأكثر أمانًا.

يتم تخزين المعلومات مثل أرقام الهواتف المحمولة وقوائم جهات الاتصال بنص عادي بدلاً من التجزئة، كما هو الحال مع الطوابع الزمنية وعناوين IP. يفشل التطبيق أيضًا في تشفير بياناتك التعريفية وأي بيانات تمت مزامنتها مع iCloud. إذا قام أي شخص باختراق السحابة الخاصة بك، فسيكون لديه إمكانية الوصول الخلفي إلى جهازك..

Telegram

الإيجابيات	السلبيات
يقدم رسائل تختفي وميزات إضافية أخرى	على الرغم من أن التطبيق مفتوح المصدر، إلا أن خوادمه ليست كذلك **(الكود مفتوح المصدر ولكن لا أحد يعلم ما يحدث داخل الخوادم إلا الشركة فقط)**
واجهة سهلة الاستخدام	التشفير ليس افتراضيًا **(عليك تفعيل الإعدادات يدوياً أو عمل محادثة مشفرة)**
	يستخدم بروتوكول التشفير الخاص

أكثر من 100 مليون شخص يستخدمون Telegram. صحيح أن المنصة سهلة الاستخدام، وتوفر العديد من الميزات الإضافية، وليست ملزمة بإعطاء أي معلومات عن المستخدم لوكالات الاستخبارات (على حد علمنا). ومع ذلك، فإن Telegram ليس آمنًا كما يريدنا أن نصدق.

أولاً، يبدو من الغريب أن تطبيق المراسلة الموجه نحو الأمان هذا لا يحتوي على تشفير افتراضيًا. العديد من الأشخاص الذين يستخدمون Telegram لا يدركون هذه المشكلة، مما يتعارض مع الغرض من التطبيق.

بروتوكول تشفير Telegram معيب أيضًا. تم تطويره من قبل فريق داخلي يتمتع بخبرة قليلة في مجال التشفير. خوادم Telegram ليست مفتوحة المصدر، لذلك لم يتم تدقيق الكود من قبل أطراف ثالثة. كما أن الشركة لا تقدم تقارير الشفافية.

(في اشارة الدراسة إلى أن تطبيق تلجرام لا يشارك المعلومات مع وكالات الاستخبارات والقول على حد علمنا بين قوسين، اشارة مباشرة إلى شكوك تدور حول التطبيق وتعاملاته مع جهات استخباراتية، ولكن بالطبع الدراسة لا يمكنها التصريح بهذا بشكل مباشرة إنما تلمح إليه)

تابع القراءة للاطلاع على أفضل ثلاثة تطبيقات للمراسلة الآمنة، أو شاهد هذا الفيديو الذي يشرح سبب اختيارنا لها.

https://www.youtube.com/watch?v=frgkHVJKVq4

Silence

الإيجابيات	السلبيات
حل آمن للرسائل النصية القصيرة/رسائل الوسائط المتعددة	لأجهزة الأندرويد فقط
مجانا للجميع	لا يوجد دعم مباشر
لا لقطة للشاشة	قاعدة مستخدمين محدودة
لا يلزم الاتصال بالإنترنت	

تطبيق Silence هو تطبيق SMS/MMS آمن يمكنك استخدامه حتى إذا لم تكن متصلاً بالإنترنت.

يمكنك إرسال رسائل إلى أي شخص، وليس فقط مستخدمين Silence .

ومع ذلك، لا يتوفر التشفير الشامل إلا عند إرسال رسائل نصية إلى مستخدمي تطبيق Silence الآخرين.

وهو متوفر على أجهزة Android فقط.

يتم تشفير جميع الرسائل المخزنة على هاتفك، ولا تتذكر لوحة المفاتيح المتخفية سجل الكتابة الخاص بك، ويمنع خيار شاشة الأمان المستخدمين من التقاط لقطات الشاشة.

من الناحية الأمنية، يعد Silence واحدًا من أكثر تطبيقات المراسلة أمانًا، ولكن إذا كنت تبحث عن ميزات أكثر تطورًا مثل مكالمات الفيديو، فسيتعين عليك البحث في مكان آخر.

Threema

الإيجابيات	السلبيات
لا يخزن البيانات أو يسجل عناوين IP	قاعدة مستخدمين محدودة
يحفظ الحد الأدنى من البيانات الوصفية	لا توجد نسخة مجانية
لا يتعين عليك تقديم البريد الإلكتروني أو رقم الهاتف للتسجيل	
الرسائل وجهات الاتصال المخزنة على جهاز المستخدم بدلاً من الخوادم	

هو تطبيق مراسلة مشفر مدفوع الأجر يوفر مستوى عالٍ من إخفاء الهوية. فهو يوفر رسائل نصية وصوتية خاصة ومكالمات صوتية ومرئية واستطلاع جماعي ومشاركة الملفات. ليس عليك حتى تقديم عنوان بريدك الإلكتروني أو رقم هاتفك للتسجيل. بدلاً من ذلك، يتم تعيين معرف تم إنشاؤه عشوائيًا. يمكنك التحقق من جهات الاتصال الخاصة بك من خلال رمز الاستجابة السريعة.

يتم حذف رسائلك من خوادم Threema بمجرد تسليمها، دون ترك أي أثر. لا يتم تخزين البيانات الوصفية، باستثناء أصغر كمية مطلوبة لتشغيل التطبيق.

بشكل عام، توفر Threema خدمات آمنة للغاية وترسل برامجها لعمليات التدقيق الخارجية لتأكيدها، مما يجعلها واحدة من أكثر تطبيقات المراسلة أمانًا على الإطلاق.

هناك عيب واحد، ربما مؤقت، وهو قلة عدد المستخدمين – حوالي 11 مليونًا فقط في الربع الأخير من عام 2022.

Wire

الإيجابيات	السلبيات
مفتوح المصدر	يجمع بعض البيانات عن مستخدميه **(عيب خطير، ليس الأفضل للخصوصية)**
يتوافق مع قوانين البيانات في الاتحاد الأوروبي	
يمكن استخدامه على غالبية متصفحات الإنترنت	

للوهلة الأولى، يحقق Wire جميع متطلبات تطبيق المراسلة الآمن - فهو يوفر تشفيرًا شاملاً، ويتوافق مع جميع قوانين البيانات والخصوصية في الاتحاد الأوروبي، كما أنه مفتوح المصدر، وليس ملزمًا بمشاركة بياناته مع خدمات المراقبة. بالإضافة إلى ذلك، يمكنك استخدامه على معظم المتصفحات الشائعة مثل Firefox وChrome وSafari وOpera. ومع ذلك، يقوم Wire بجمع وتخزين بعض بيانات المستخدم.

اعترف منشئوا التطبيق بالاحتفاظ بسجلات للأشخاص الذين اتصل بهم المستخدمون، ولسوء الحظ يتم حفظها كلها بنص عادي. كما يقوم أيضًا بتخزين عناوين البريد الإلكتروني للمستخدمين وأرقام هواتفهم وأسماء المستخدمين. ووفقا لـ Wire، فإن هذه المعلومات تجعل مزامنة الجهاز أسهل ويتم حذفها بمجرد إلغاء تنشيط الحساب.

Wickr

الإيجابيات	السلبيات
لا تحتاج إلى رقم هاتف أو عنوان بريد إلكتروني للتسجيل	قد يكون من الصعب التبديل من منصات المراسلة الأخرى اليه
مفتوح المصدر	
يقدم ميزة "التقطيع"	
لا يجمع بيانات المستخدم أو يخزن البيانات الوصفية	
يقدم نسخة برو للشركات	

يعد Wickr أحد أفضل تطبيقات المراسلة الآمنة في السوق. إنه مفتوح المصدر ولا يجمع بيانات المستخدم أو البيانات الوصفية. كما يوفر أيضًا ميزة "التقطيع"، التي تقوم تلقائيًا بحذف جميع المحادثات والملفات التي تمت مشاركتها على النظام الأساسي.

يمكنك ضبط مؤقت لوقت حذفها. والأهم من ذلك، أنك لا تحتاج إلى رقم هاتف أو عنوان بريد إلكتروني للتسجيل، لذلك من الأسهل الحفاظ على خصوصية حياتك.

الجانب السلبي الوحيد هو أن Wickr لا يحظى بشعبية مثل Signal أو Telegram. تم تصميمه في البداية للشركات والمؤسسات، لذلك لم يتم الإعلان عنه على نطاق واسع للمستخدمين العاديين.

لا يزال Wickr يقدم إصدار Pro مدفوع حيث يمكنك إجراء مكالمات فيديو جماعية مشفرة، وهو شيء لا يقدمه أي تطبيق آخر حاليًا.

إذا لم تكن رائد أعمال وترغب في استخدام Wickr، فستحتاج إلى إقناع أصدقائك بالتحرك أيضًا.

Signal

الإيجابيات	السلبيات
يتعامل مع الدردشات الجماعية والرسائل النصية القصيرة والصوت والفيديو والمستندات والرسائل المصورة	يحتاج إلى رقم هاتف للتسجيل **(ليس عيب خطير حيث يمكن استخدام الرقم الوهمي)**
يقدم رسائل تختفي (مع مؤقت)	
بروتوكول الإشارة	
مفتوح المصدر	
لا يخزن بيانات المستخدم أو البيانات الوصفية	
دافع عنه إدوارد سنودن	

هو الأفضل من بين باقي التطبيقات لكل من مستخدمي iOS وAndroid.

أنشأ Signal بروتوكول تشفير يُعرف الآن بأنه بروتوكول تطبيق المراسلة الأكثر أمانًا المتاح. إنه يوفر كل ما يحتاجه معظم المستخدمين - الرسائل القصيرة ومكالمات الفيديو والصوت والمحادثات الجماعية ومشاركة الملفات واختفاء الرسائل - دون حشو التطبيق بالإعلانات وجمع بيانات المستخدم.

إنها أيضًا منصة مفتوحة المصدر بحيث يمكن لأي شخص التحقق من نقاط الضعف فيها.

بالحديث عن ذلك، ربما عثرت شركة أمنية إسرائيلية على ثغرة أمنية محتملة، ولهذا السبب من الأفضل دائمًا استخدام VPN جنبًا إلى جنب مع تطبيقات المراسلة الآمنة المفضلة لديك.

(الدراسة هنا تشير إلى تطبيق بيجاسوس الإسرائيلي)

المقارنة بين التطبيقات



Comparison						wickr				
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓	–	–	–
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓	✓	✗	–
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Open source apps	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Open source servers	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Personal information is hashed	✗	✗	✗	✗	–	✓	–	✓	–	–
Encrypts metadata	✗	✗	✗	✗	–	✓	✓	–	–	–
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	–	✓	✓	✓	–	–

رفض التعاون مع وكالات الاستخبارات، يقدم تقارير الشفافية، يمتنع عن جمع بيانات المستخدم، التشفير الافتراضي، تطبيقات مفتوحة المصدر، خوادم مفتوحة المصدر، تتم تجزئة المعلومات الشخصية، البيانات الوصفية المشفرة، لا يسجل الطوابع الزمنية وعناوين IP

في الصورة أعلاه لاحظ أن تطبيقات مثل ماسنجر فيس بوك وواتس أب مثلا مشهورة جداً بتعمالها مع أجهزة الإستخبارات وتقديم البيانات لهم عند طلبها.

لاحظ كذلك أن تطبيق مثل سينجنال قد اجتاز جميع الإختبارات الأمنية بنجاح وحقق جميع المتطبيات.

هل تحتاج إلى تطبيق مراسلة مشفر؟

نعم، أنت بحاجة إلى استخدام أحد أفضل تطبيقات المراسلة المشفرة لأن التشفير يحمي اتصالاتك من الاعتراض. يمكن للأطراف الثالثة قراءة الرسائل غير المشفرة بسهولة، بينما تتمتع الرسائل المشفرة بطبقة إضافية من الحماية.

التشفير من طرف إلى طرف (E2E) يعني أن مستلمي الرسالة فقط هم من يمكنهم قراءتها لأنهم الوحيدون الذين لديهم مفتاح فك التشفير.

مع وجود العديد من التهديدات عبر الإنترنت التي تعرضنا للخطر، فمن الحكمة استخدام أحد تطبيقات المراسلة الأكثر أمانًا. من المحتمل أن معظم من حولك يستخدم واحدًا، لذلك عليك فقط أن تقرر أي واحد تختاره، بناءً على الأوصاف المذكورة أعلاه.

نصائح حول كيفية تأمين تطبيق المراسلة الخاص بك

تعد الرسائل المشفرة أكثر أمانًا من الرسائل غير المشفرة، ولكن لا يزال يتعين عليك توخي الحذر عند استخدام تطبيقات المراسلة الأكثر أمانًا. اتبع قائمة التحقق هذه للحفاظ على حماية تطبيق المراسلة الخاص بك:

أولاً: كن حذرًا عند استخدام شبكات Wi-Fi العامة. تفتقر هذه الشبكات عادة إلى التدابير الأمنية الأساسية، مما يجعل من السهل على المتسللين التطفل على حركة مرور الويب الخاصة بك.

إذا كنت تستخدم خدمة مراسلة غير مشفرة على شبكة Wi-Fi عامة، فيمكن لمجرمي الإنترنت اعتراض رسائلك وصورك وكلمات مرورك والمعلومات الحساسة الأخرى التي تشاركها. يمكن أن تساعد شبكة VPN الآمنة في حمايتك عن طريق إخفاء حركة المرور الخاصة بك عن المتلصصين ومنع الخروقات الأمنية.

ثانياً: لا تقدم معلومات خاصة من خلال المحادثات. تجنب مشاركة كلمات المرور والمعلومات المصرفية وتسجيلات الدخول وأي معلومات حساسة أخرى من خلال الدردشات. ولا تشارك أبدًا هذا النوع من المعلومات مع الغرباء.

ثالثاً: لا تنقر على الروابط المشبوهة. إذا أرسل إليك شخص لا تعرفه رسالة نصية وأرسل لك رابطًا يبدو بريئًا، فلا تنقر عليه. يُعرف المحتالون عبر الإنترنت بإرسال روابط عشوائية إلى مواقع التصيد الاحتيالي.

رابعاً: استخدم VPN موثوقًا. فهو يقوم بتشفير حركة مرور التطبيق وحركة المرور عبر الإنترنت بشكل فوري وقوي.

يتم تمويل شبكات VPN المدفوعة مثل NordVPN بشكل أفضل للبحث والتطوير في طرق التشفير، لذلك نضمن لك مستوى أعلى من الأمان داخل وخارج التطبيقات التي تستخدمها. تعمل ميزة الحماية من التهديدات الإضافية في NordVPN على الارتقاء بأمانك إلى المستوى التالي من خلال حظر الإعلانات وأجهزة التتبع والبرامج الضارة. كما أنه يقوم بفحص ملفاتك بحثًا عن البرامج الضارة أثناء التنزيل، لذلك يمكنك الاطمئنان إلى أن جهازك لن يصاب بالعدوى حتى إذا قمت بالنقر فوق رابط مشبوه عن طريق الصدفة.

(هنا قامت شركة NordVPN بالتوصية بنفسها في الدراسة كونها من عملت عليها، ولكن هذا لا يعني أنها الأفضل بين تطبيقات VPN، راجع الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنوان – أفضل خدمات VPN 2023 – للمزيد من التفاصيل حول VPN)

لماذا يجب عليك دائمًا استخدام VPN

التشفير التام بين الطرفين ليس مضمونًا. يتم استغلال الأبواب الخلفية داخل التطبيقات المشفرة طوال الوقت. في عام 2020، أعلنت شركة Cellebrite الأمنية (التي يستخدمها مكتب التحقيقات الفيدرالي وشرطة ميانمار والحكومات) أنها تمكنت من التحايل على التشفير الشامل لتطبيق Signal.

تم تحذير WhatsApp بشأن افتقاره إلى النسخ الاحتياطية المشفرة من طرف إلى طرف، وإذا لم تجعل محادثات Telegram الخاصة بك "سرية"، فلن يتم تشفيرها. لذلك، أيًا كان تطبيق المراسلة المشفر الذي تختاره، اجعله أكثر أمانًا عن طريق تشغيل تطبيق NordVPN، الذي يخفي حركة المرور الخاصة بك على الفور عن المتلصصين الذين قد يتربصون في الشبكة.

(هنا قامت شركة NordVPN بالتوصية بنفسها في الدراسة كونها من عملت عليها، ولكن هذا لا يعني أنها الأفضل بين تطبيقات VPN، راجع الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنوان – أفضل خدمات VPN 2023 – للمزيد من التفاصيل حول VPN)

مع تحيات إخواكم في جيش الملاحم الإلكتروني

و

مجلس التعاون الإعلامي الإسلامي

تتصح بمراجعة كتاب الحرب الإلكترونية الجزء الأول – الأمن السيبراني –

من إعداد مجلس التعاون الإعلامي الإسلامي

كما ننصح بمراجعة الدراسة السابقة الصادرة عن جيش الملاحم الإلكتروني بعنون

– أفضل خدمات VPN 2023 –

أفضل محاكيات Android لأجهزة الكمبيوتر التي تعمل بنظام Windows لعام 2023

إعداد: مجلس التعاون الإعلامي الإسلامي

تقديم: جيش الملاحم الإلكتروني



Al-Malahem Electronic Army

بسم الله الرحمن الرحيم

جيش الملاحم الإلكتروني

يقدم

*** دراسة ملحقة: أفضل محاكيات Android لأجهزة الكمبيوتر التي تعمل بنظام Windows لعام 2023 ***

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

المصدر

https://www.guru99.com/best-android-emulators-mac-windows.html

مقدمة مجلس التعاون الإعلامي الإسلامي

تستخدم المحاكيات من عوام الناس لغايات الألعاب الإلكترونية في المقام الأول، ولكن يمكن لك استخدامها في العديد من المجالات فهي تسمح لك عمل أي عدد تريده من الهواتف الوهمية في جهاز كمبيوترك الخاص لتستخدمها كما تستخدم الهواتف.

فإن جميع ما يمكنك فعله في الهاتف الحقيقي يمكنك فعله في الهاتف الوهمي عبر المحاكيات.

رغم أن أغلب دراسات المحاكيات سوف تهتم في مجال الألعاب بالمقام الأول بما في ذلك هذه الدراسة المترجمة، إلا أننا ننبه إلى أننا لا نشجع على ممارسة هذا النوع من إهدار الوقت بلا فائدة، ولكننا سوف نقدم الدراسة مترجمة كما هي ويمكنك تحديد نوع المحاكي الذي تستخدمه منطلقاً من ذات المفاهيم (القوة، الأمان، التحديث، دعم أحدث الإصدارات ....)

قبل المضي قدماً في الدراسة ننصحك بمواصلة القراءة في هذا الفصل المنقول عن فصل: الحماية من التتبع والمحاكيات وطبقات الحماية.

كتاب الحرب الإلكترونية – الجزء الأول – الأمن السيبراني

صادر عن: مجلس التعاون الإعلامي الإسلامي

إن تم إختراق جهازك، فلن تنفعك أغلب وسائل الحماية المتبعة.

وذلك لأن المخترق سوف يقوم بفتح باب خلفي (منفذ خلفي أو بورت خاص) داخل جهازك سوف يقوم بسرقة معلومات الجهاز وكل ماتفعله قبل أن يتم تشفيره من الأساس ويرسل نسخة منه إلى المخترق، كذلك سوف يستمر بمتابعة عناوين الآي بي الخاصة بك العامة والخاصة ويرسل تحديثات مستمرة لها، فأغلب وسائل الحماية لن تكون مفيدة في هذه الحالة. لذلك فإننا ننصح بحماية جهازك أولاً.

- كيف أحمي جهازي أولاً؟

ليس من السهل حماية جهازك الشخصي، بالتأكيد مطلوب منك تركيب برمجيات الحماية من الفيروسات، والجدار الناري لمنع الاختراق، تطبيقات الفي بي ان لإخفاء "الاي بي" وفحص البورتات أو المنافذ باستمرار مع إغلاق ومنع مرور البيانات من الغير مستخدم أو المشبوه منها.

ورغم هذا كله يمكن اختراق الجهاز، فالعدو متقدم تقنياً للغاية.

أول توصية نوصي بها هي عدم استخدام جهاز من الأصل، التوقف تماماً عن استخدام الهواتف النقالة، واستبدالها بأجهزة اللابتوب مع استخدام محاكيات الجوالات.

الأجهزة يجب ان تكون بمعالج قوي وبنفس الوقت صغيرة الحجم يمكن حملها بسهولة، والأهم هو مع عدم وجود كميرا داخلها وعدم وجود نظام المواقع الجغرافية "الجي بي أس".

هذه الأجهزة متوفرة بالسوق، يكفي ان تطلب جهاز بمواصفات محدده، بدون كميرا وبدون جي بي أس، ولعدم إثارة شكوك البائع اقرأ جيداً مواصفات الجهاز واحرص على أن لا يكون من بينها نظام التتبع الجغرافي ولا الكاميرا.

وفي حال تعذر الحصول على جهاز بدون كميرا، يمكن تغطيتها ببساطة بالطريقة التقليدية، بينما لا تقتني ابداً جهاز مدمج فيه نظام التتبع الجغرافي "الجي بي أس".

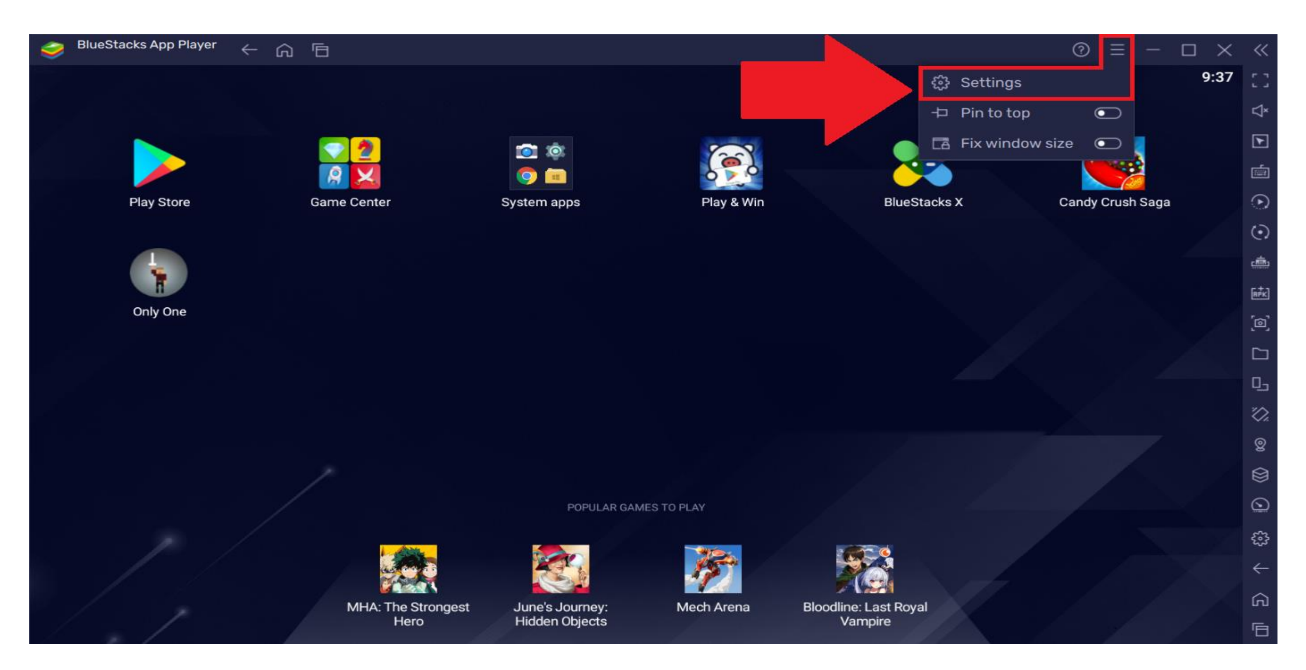
- كيف سوف استخدم تطبيقات الهاتف الجوال من خلال اللابتوب؟

لا تستخدمها مباشرة، فالتلجرام وجميع التطبيقات تقدم نسخة لنظام تشغيل ويندوز أو باقي أنظمة تشغيل اللابتوبات، ولكن لا تستخدمها.

عليك استخدام محاكيات الجوال...

وهي تطبيقات برمجية تقوم بتحميلها على اللابتوب، تسمح لك بعمل أجهزة خلوية وهمية في جهازك، بالعدد الذي تريده.

على سبيل المثال المحاكي التالي BlueStacks x
https://www.bluestacks.com
من أكثرها شهرة، ولكنك غير ملزم باستخدام هذا المحاكي تحديداً، يمكنك البحث عن بديل له.



يمكنك من خلال محاكيات الجوال عمل أي عدد تريده من الهواتف الوهمية داخل جهاز الكمبيوتر الخاص بك متجاوزاً كل المخاطر المترتبة على استخدام الهاتف التقليدي

بعد عمل الهواتف الوهمية في جهاز اللابتوب سوف تنتقل حماية اللابتوب إلى الهواتف الوهمية تلقائياً، أي أن كل مكافح فيروسات وبرنامج في بي أن تستخدمه فهو سوف يحمي اللابتوب بما فيه المحاكيات.

حيث بالطبع ستكون قد قمت بتركيب مكافح الفيروسات، الجدار الناري، الفي بي أن، حماية الشاشة.

وبشكل تلقائي سوف تعمل حماية اللابتوب على حماية الهواتف الوهمية.

ولكن كطبقات إضافية للحماية، يمكنك التعامل مع الهاتف على أنه غير وهمي، وقم فيه بتركيب مكافح فيروسات، وجدار ناري، وفي بي أن وحامي شاشة خاص به.

الأمر جيد، كلما قمت بتركيب طبقات حماية أكثر فهذا أفضل. بالطبع يعتمد على سرعة معالج اللابتوب ومواصفاته بالإضافة لسرعة شبكة الأنترنت عندك.

وبالطبع بت تدرك الآن أن تطبيق الهواتف الوهمي هو بحد ذاته طبقة حماية إضافية.

لا أريد التوصية بتطبيقات محددة، بل الأفضل أن يقوم جميع الإخوة بالبحث بأنفسهم، السبب أنهم خلال بحثهم سوف يقرأون أكثر، ويفهمون أكثر، ويتعلمون أكثر.

حسناً الآن تصور معي هذا المشهد ...

أنت تستخدم محاكي جوالات في اللابتوب، يوجد داخل الهاتف الوهمي في بي أن من شركة روسية، ومكافح فيروسات من شركة صينية، وجدار ناري وحامي شاشة.

ثم في اللابتوب نفسه تستخدم في بي أن من شركة كورية، مكافح فيروسات من شركة أخرى، جدار ناري وحامي شاشة ....

ثم أرسلت رسالة عبر تطبيق مشفر بالكامل End to End

مرحباً بك في عالم التعقيد ....

إن وقعت حزمة رسالتك هذه بيد جهة ما في العالم وكذب تطبيق التشفير وقام بفك تشفيرها، سوف يصطدم بتشفير شركة في بي أن الهاتف الوهمي، سيذهبون لها، ستفك التشفير، سوف تصطدم بتشفير شركة الفي بي أن في اللابتوب ... الخ

حسناً ماذا لو تم اختراق الهاتف الوهمي؟ سوف يصطدمون بحماية اللابتوب نفسه.

باقي الهواتف الوهمية في أمان تام.

وعليه فإننا ننصح في الهواتف الوهمية أن لا تقوم بجعل كل عملك في هاتف واحد فقط، قسمها، باختصار أجعل من سوف يوقع بك يذوق الأمرين قبل التمكن من هذا إن استطاع.

ولكن بطبيعة الحال فإن هناك نصيحة هامة لا تتجاهلها فيما يتعلق في الفي بي أن

نصحك بالإبتعاد عن التطبيقات المجانية

هذا الأمر غاية بالضرورة، خصوصاً في مكافح الفايروسات والجدار الناري والفي بي أن.

استخدموا التطبيقات الرسمية المباعة، واختاروا تطبيقات من شركات ودول مختلفة كما ورد شرحه سابقاً، وادفعوا ثمن الخدمة من خلال العملات المشفرة "البتكوين".

- ليس لدي لابتوب، لا يمكنني الحصول عليه الآن، هل يوجد بديل للمحاكيات مخصص للهواتف؟

نعم يوجد ولكن ليس بنفس القوة والكفاءة، سوف يتم شرحها.

- ماذا لو سقط جهازي بيد العدو؟

هنا تأتي مرحلة الإبتكار. حيث يمكنك ابتكار طرق حماية إضافية.

شخصياً لا أوصي أبداً أن تكون جميع ملفاتك على اللابتوب، بل يكون جهاز اللابتوب مجرد وسيلة فقط.

بينما تقوم بتركيب تطبيقات الهواتف الوهمية وكل ما يلزمك من تطبيقات أخرى على ذاكرة خارجية "فلاش مثلاً" بسعة عالية جداً 1 تيرا بايت مثلا أو 500 جيجا.

وبمجرد سحب هذا "الفلاش" من الجهاز فعندها يصبح فارغ بلا فائدة لأي جهة كانت.

والجميل في هذا الأمر أن بمقدورك أن تعود وتستخدم هذا "الفلاش" في أي جهاز آخر.

بالطبع الذاكرة الخارجية لابد أن تكون محمية بنظام تشفير، لذلك عند اختيارها اختر نوع الذاكرات الذي يكون محمي بكلمة مرور، او قم بتركيب نظام تشفير عليها.

في أسوأ الأحوال، إذا تعرضت للمداهمة، كل ما يلزم الأمر هو إخراج "الفلاش" في ثانية واحدة ثم تكسيرها أو رميها في مكان يصعب الوصول إليه.

- هل من إجراءات اضافية؟

بالطبع، الحماية عالم لا ينتهي، والابتكار هو مفتاح النجاح بها.

قد يأتي أخ الآن ويستنبط ويبتكر فكرة جديدة من الشرح أعلاه تقوي من بروتوكولات الحماية هذه.

المقدمة

محاكي Android هو تطبيق برمجي يسمح لهاتفك المحمول بتقليد ميزات نظام التشغيل Android على جهاز الكمبيوتر الخاص بك، يسمح لك بتثبيت تطبيقات Android على جهاز الكمبيوتر أو الكمبيوتر المحمول الخاص بك واستخدامها في جهازك، يتم استخدامه بشكل رئيسي لأغراض التصحيح.

فيما يلي قائمة منتقاة بعناية من أفضل محاكيات Android، مع ميزاتها الشائعة وروابط مواقع الويب الخاصة بها.

تحتوي القائمة على برامج مفتوحة المصدر (مجانية) وتجارية (مدفوعة).

أفضل محاكي Android لأجهزة الكمبيوتر التي تعمل بنظام Windows وMac

المحاكي	المنصة	السعر	الموقع الإلكتروني
BlueStacks	Windows, and macOS	مجاناً بالكامل	https://www.bluestacks.com
LDPlayer	Windows	مجاناً بالكامل	https://www.ld-space.com
NoxPlayer	Windows, Android and iOS	يتوفر نسخة مجانية أساسية	https://www.bignox.com
Memu	Android, iOS, Windows and Mac	يتوفر نسخة مجانية أساسية	https://www.memuplay.com
Genymotion	Windows, Linux and Mac	مجاناً ل 30 يوم فقط	https://www.genymotion.com

BlueStacks



يعتبر BlueStacks المملوك من قبل now.egg, Inc مشغل التطبيقات رقم 1 في العالم لأجهزة الكومبيوتر المكتبي وال Mac.

إنه مصمم للاعبين ويوفر أداءً فائقًا وعناصر تحكم دقيقة في اللعبة باستخدام لوحة المفاتيح والماوس أو لوحة الألعاب.

واحدة من أكبر نقاط القوة في BlueStacks هي أنه يوفر تخصيصات خاصة باللعبة تعزز تجربة اللعب واللعبة، وهو أيضًا مشغل التطبيقات الوحيد الذي يتمتع بدعم Android 11.

إلى جانب ذلك، يمكنك الاستمتاع بما يصل إلى 240 إطارًا في الثانية من اللعب، أو اللعب محليًا أو على السحابة، وهي أسرع وأخف منصة ألعاب على الإطلاق.

يتوفر BlueStacks لنظام التشغيل Microsoft Windows 10 (الإصدار 1903 وما فوق)، وWindows 11، وMac، مما يتيح للاعبين تجربة الألعاب الشهيرة مثل State of Survival وMARVEL Strike Force وSquad RPG بمعدل يصل إلى 240 إطارًا في الثانية.

ومع الحد الأدنى من متطلبات النظام المتمثلة في درجة اختبار وحدة معالجة الرسومات >= 750 وذاكرة الوصول العشوائي (RAM) سعة 4 جيجابايت، فإنه يضمن أن اللعب الخاص بك سلس وسريع الاستجابة.

BlueStaks هي أداة متعددة الإستخدامات وتوفر ميزات اللمس المتعدد بالاضافة الى دعم ARM ومستوى البطارية مما يعزز تجربة تطبيق Android على جهاز الكومبيوتر مع الأداء والكفاءة الأمثل. تعتبر هذه الأداة مثالية للألعاب الإلكترونية عالية المستوى دون الحاجة الى اجهزة متطورة.

المواصفات

- يمكنك لعب عدة ألعاب في وقت واحد
- يدعم نظام Android 11
- تسجيل وإعادة تشغيل أي إجراء في الوقت الحقيقي
- يقدم دعمًا أصليًا للوحة الألعاب، وأوضاع الأداء، وذاكرة القطع، والبرنامج النصي، وإطارًا عاليًا في الثانية
- يعمل على Android 9، 10، 11، 12، 13 وأحدث إصدارات Android
- يوفر دعم العملاء عبر البريد الإلكتروني والدردشة وReddit وDiscord
- الأنظمة الأساسية المدعومة: Windows وmacOS

الإيجابيات

- يمكنك تشغيل جميع تطبيقات Android تقريبًا باستخدام هذا الجهاز
- متكاملة مع اللعب والفوز، يمكن للمرء الفوز بجوائز مثيرة من خلال القيام بالمهام
- سهل الاستخدام والإعداد، مع تصميم أنيق وواجهة مستخدم
- يمكنه تشغيل حالات متعددة
- يمكن لعب عدة ألعاب في نفس الوقت
- دعم لحسابات متعددة

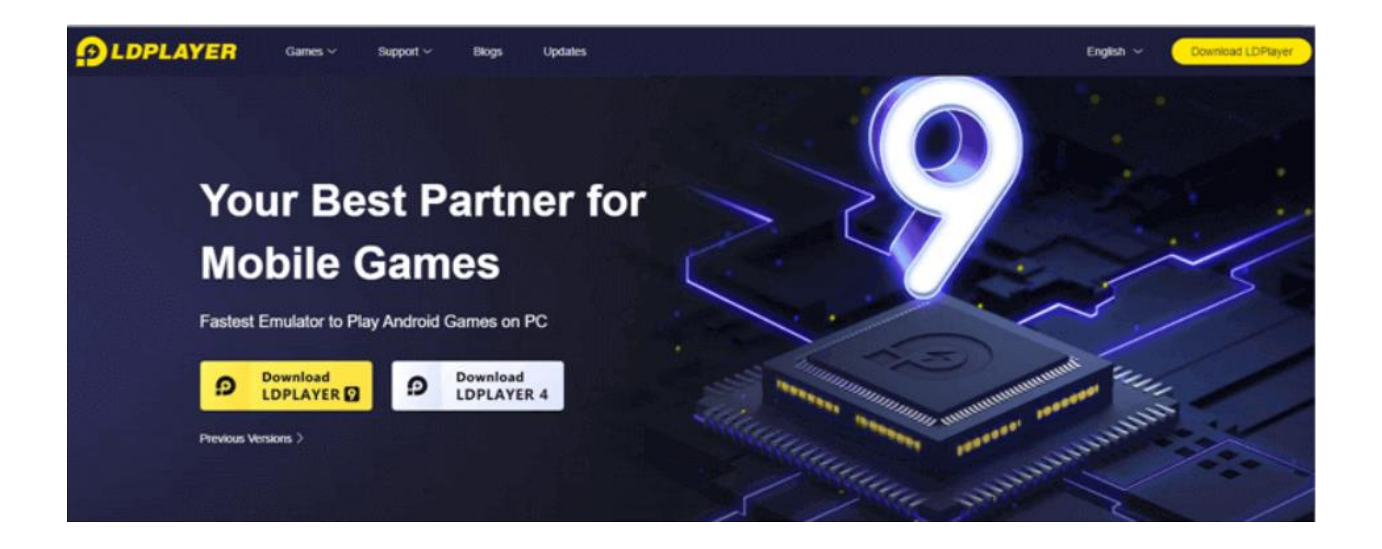
السلبيات

- قد لا يعمل بشكل جيد على أجهزة الكمبيوتر الشخصية أو أجهزة الكمبيوتر المحمولة المنخفضة الجودة
- يتم تضمين الإعلانات في التطبيق ولكنها تأتي مع خيار تعطيلها

السعر

- هي أداة متعددة الاستخدامات تقدم نسخة تجريبية مجانية مدى الحياة. استمتع بلعب تطبيقات وألعاب Android على جهاز الكمبيوتر، مما يضمن تحسين الأداء واللعب.

LDPlayer



يقدم LDPlayer نظام محاكاة Android مثاليًا، فهو يوفر الكثير من الميزات الشاملة لتلبية كل ما يتم تنفيذه بواسطة أي جهاز يعمل بنظام Android.

يمكنك الوصول إلى الألعاب والتطبيقات من متجر LD Store أو Google Play.

يوفر LDPlayer اللمس المتعدد ودعم ARM وحالة البطارية في الوقت الفعلي، مما يضمن تجربة مستخدم سلسة وفعالة وسريعة الاستجابة للألعاب المحمولة على الكمبيوتر.

LDPlayer هو محاكي Android غني بالميزات يسمح لك بلعب الألعاب الشهيرة مثل Arknights وGarena Free Fire وClash of Clans على جهاز الكمبيوتر الخاص بك.

وهو يدعم وظائف متنوعة، بما في ذلك تعليمات الوظيفة، ونموذج الهاتف الافتراضي، وجسر الشبكة.

تأكد من أن جهاز الكمبيوتر الخاص بك يحتوي على ذاكرة وصول عشوائي لا تقل عن 2 جيجابايت ومجهز بمعالج NVIDIA GeForce أو Intel أو AMD Processor x86/x64 لتحسين الأداء.

المواصفات

- يساعدك على إدارة ألعابك تلقائيًا
- يوفر تحكمًا مخصصًا باستخدام لوحة المفاتيح والماوس
- يسمح لك بفتح العديد من الألعاب في وقت واحد
- متوفر لنظام التشغيل Windows XP XP3 / Win7 / Win8 / Win8.1 / Win10
- يعمل على أندرويد 3.0، 4.0، 9.0 أو أعلى
- يوفر دعم العملاء عبر البريد الإلكتروني
- المنصات المدعومة: Windows

الإيجابيات

- سرعة التنفيذ سريعة والكود خفيف الوزن
- التحديثات متوفرة على أساس منتظم
- طريقة سهلة للوصول إلى الاختصارات لنظام Android
- يدعم التغيير والتبديل في تخصيص الموارد

السلبيات

- تبدو جودة الصوت منخفضة
- لعبة ببجي موبايل لا تعمل بسلاسة

السعر

- LDPlayer هو محاكي Android مجاني يعمل على تحسين أداء الألعاب على أجهزة الكمبيوتر. مع النسخة التجريبية المجانية مدى الحياة، استمتع بألعاب الهاتف المحمول مع تحكم محسّن.

NoxPlayer



Nox Player هو محاكي Android آخر معترف به من قبل محبي الألعاب حول العالم.

يمكنك تشغيل هذا المحاكي على أجهزة مختلفة تسمح بتشغيل وظائف متعددة.

تعتبر هذه الأداة رائعة للاعبين الذين يهدفون إلى الحصول على تجربة ألعاب Android مثالية على أجهزة الكمبيوتر الخاصة بهم.

يوفر NoxPlayer حالة البطارية، واللمس المتعدد، ودعم ARM، مما يضمن تجربة محاكاة Android فعالة وسهلة الاستخدام وسريعة الاستجابة.

يتيح لك NoxPlayer، المتوفر للأنظمة الأساسية التي تتراوح من Windows XP SP3 إلى Win10، ممارسة الألعاب الشهيرة مثل Mobile Legends وSummoners War وState of Survival. يعمل على نظام التشغيل Android 5، 7، 9 أو أعلى، مما يضمن التوافق مع التطبيقات المختلفة. ضع في اعتبارك الحد الأدنى لمتطلبات النظام: رسومات NVIDIA وAMD وذاكرة الوصول العشوائي (RAM) سعة 1.5 جيجابايت.

المواصفات

- إنه أحد أفضل المحاكيات للكمبيوتر الشخصي الذي يوفر تعيينًا مفتوحًا للوحة المفاتيح يعمل بنقرة واحدة، وجميع عناصر التحكم في الألعاب على الماوس ولوحة المفاتيح
- يأتي مشغل Nox مزودًا بمسجل ماكرو افتراضي لتسجيل العمليات المعقدة.
- يقدم أفضل تجربة للمستخدم والأداء المتفوق
- عروض تخصيص اللعبة الخاصة بك، ولعب ألعاب مختلفة في نفس الوقت، ومحركات الأقراص المتعددة وتسجيل البرنامج النصي
- يوفر دعم العملاء عبر الهاتف والبريد الإلكتروني
- الأنظمة الأساسية المدعومة: ويندوز، أندرويد، وiOS

الإيجابيات

- سريع وسهل الاستخدام وقابل للتخصيص بدرجة كبيرة
- يتم توفير تجربة مستخدم رائعة من خلال هذا التطبيق
- يدعم استخدام عصا التحكم واللوحة التفصيلية
- التحديثات وإصلاح الأخطاء بشكل منتظم
- يدعم مثيلات متعددة ونوافذ متعددة على جهاز واحد
- رسم خرائط الاختصارات على وحدات التحكم

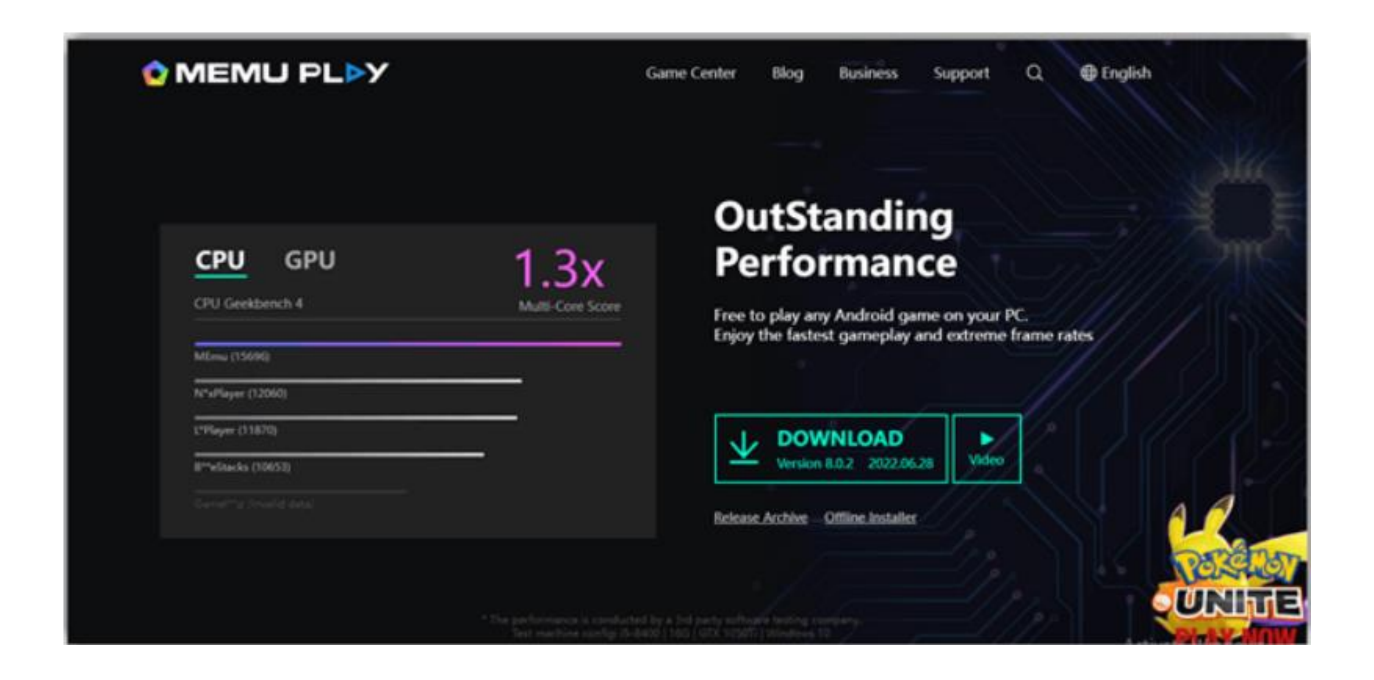
السلبيات

- يكون بطيئًا عند فتح عدة نوافذ في نفس الوقت
- البروتوكولات الأمنية سيئة

السعر

- يقدم NoxPlayer خطة أساسية مجانية مدى الحياة. بالنسبة للميزات المتقدمة، تبدأ الحزمة بسعر 14.49 دولارًا شهريًا، مما يوفر تجارب محسنة للألعاب والمهام المتعددة.

Memu



من السهل تثبيت تطبيق Memu لمحاكاة Android.

إنه أحد أفضل محاكيات Android للكمبيوتر الشخصي والذي يقدم الدعم لرقائق Intel وAMD، بالإضافة إلى الرسومات المدمجة والمخصصة.

Memu هو محاكي Android مزود بتقنية اللمس المتعدد ودعم ARM وميزات حالة البطارية، مما يوفر تجربة هاتف محمول سلسة على جهاز الكمبيوتر.

يتوفر Memu لأنظمة WinXP SP3 وWin7 وWin8 وWin10 ويتيح لك ممارسة الألعاب الشهيرة مثل Garena Free Fire وPUBG MOBILE وCall of Duty Mobile.

يعمل بنظام التشغيل Android 7 أو أعلى، ويتضمن الحد الأدنى لمتطلبات النظام وحدة تحكم Intel/Nvidia/ATI مع درجة PassMark > 750 وذاكرة وصول عشوائي (RAM) سعة 2 جيجابايت. ومع ذلك، من الضروري التأكد من أن نظامك يلبي هذه المتطلبات للحصول على الأداء الأمثل.

المواصفات

- مجموعة من خيارات تعيين لوحة المفاتيح لتحسين تجربة الألعاب الخاصة بك
- توفير خيار للمحاكاة الافتراضية
- يوفر العديد من إعدادات لوحة المفاتيح المخصصة لتجربة اللعب السريعة
- يقدم تصميمًا جديدًا لواجهة المستخدم لتجربة مستخدم أفضل، وترقية المحرك الأساسي وتحسينًا رائعًا، والتحسين النهائي وكفاءة الإدارة
- يوفر دعم العملاء عبر البريد الإلكتروني ونموذج الاتصال
- الأنظمة الأساسية المدعومة: Android، وiOS، وWindows، وMac

الإيجابيات

- تتوفر ميزة تعيين المفاتيح المخصصة
- يقوم بإعداد موقعك الافتراضي على خرائط جوجل
- يدعم كلا من بطاقات الرسوميات AMD و NVidia
- يقوم بتثبيت ملفات APK بنقرة واحدة
- فيما يتعلق بأداء الألعاب، فهو جيد حقًا

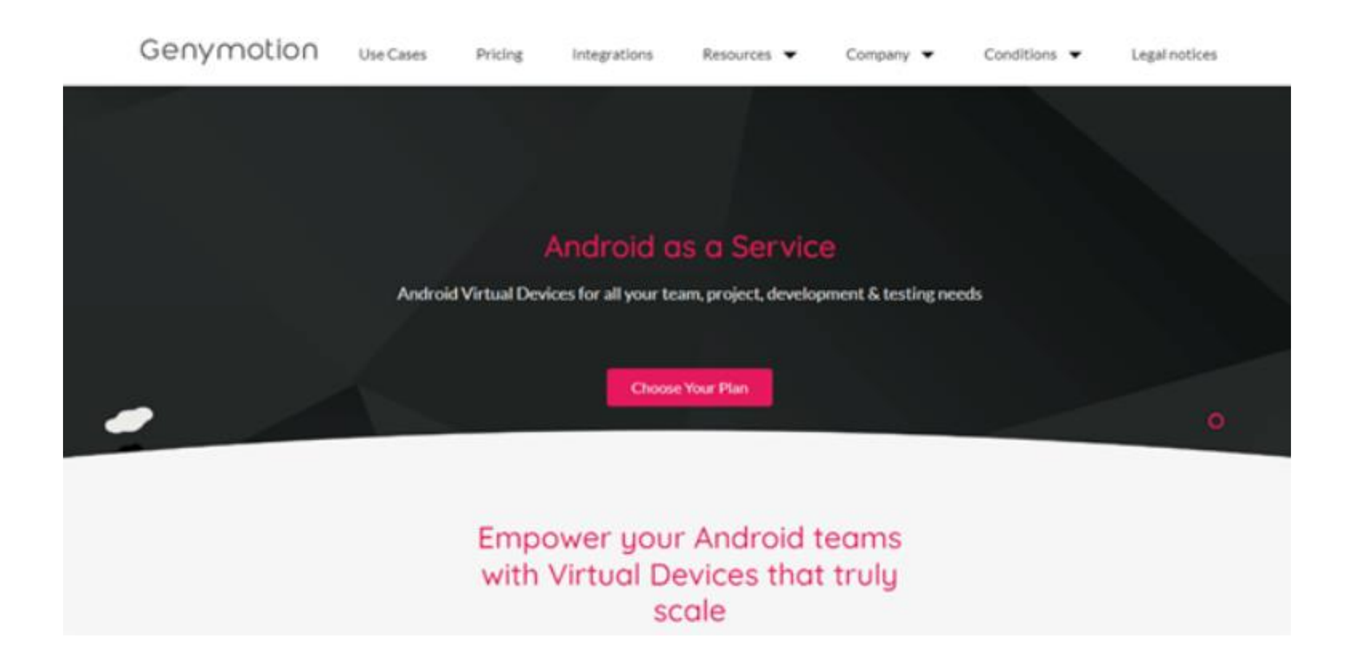
السلبيات

- لا يعمل بشكل جيد على أجهزة الكمبيوتر الضعيفة
- يقتصر على الألعاب فقط
-

السعر

- تقدم Memu خطة أساسية مجانية مدى الحياة للمستخدمين. بالنسبة للميزات المتقدمة، تبدأ الحزمة بسعر معقول يبلغ 2.99 دولارًا شهريًا، مما يوفر تنوعًا وأداءً محسنًا.

Genymotion



Genymotion هو محاكي Android متعدد الدعم. يساعدك البرنامج على تسريع الاختبار ومشاركة العروض التوضيحية المباشرة. يمكنك أيضًا مراقبة الأداء عبر جميع الأجهزة.

يعد Genymotion واحدًا من أفضل برامج محاكاة Android لنظام Linux، مما يسمح للمستخدمين باختبار المنتجات في بيئة افتراضية آمنة. هذه الأداة، المتوفرة أيضًا لأنظمة التشغيل Windows 8 و8.1 و10 وLinux Ubuntu 18.04LTS أو LTS20.04، قادرة على محاكاة أكثر من 3000 تكوين Android، مثل الإصدار وحجم الشاشة، فهو يوفر التوافق ومحاكاة سياق المستخدم وإجراءاته والأداء، مما يضمن نطاقًا واسعًا من الاختبارات.

ضع في اعتبارك أن التثبيت يتطلب وحدات معالجة الرسومات NVIDIA أو AMD وما لا يقل عن 4 جيجابايت من ذاكرة الوصول العشوائي، ويعمل على Android 4.4 أو أعلى.

المواصفات

- يوفر توافقًا عالي الدقة للبكسل، مما يوفر وضوحًا أفضل على جهاز الكمبيوتر الخاص بك.
- يسمح لك باستخدام كاميرا ويب سطح المكتب كمصدر فيديو لتسجيل لقطات الشاشة
- يحتوي محاكي Android لنظام التشغيل Mac هذا على أجهزة استشعار قوية، مثل نظام تحديد المواقع العالمي (GPS) واللمس المتعدد
- يوفر دعم العملاء عبر الدردشة ونموذج الاتصال
- الأنظمة الأساسية المدعومة: ويندوز، لينكس، وماك

الإيجابيات

- أفضل محاكيات الأندرويد للمطورين
- يدعم مجموعة واسعة من إصدارات أندرويد
- يدعم اندرويد ستوديو
- يدعم أيضًا اللمس المتعدد، ARM
- تتوفر مكتبة كبيرة من الأجهزة المقلدة والمخصصة

السلبيات

- غير مناسب للألعاب
- لم يتم تضمين متجر Play

السعر

- يوفر Genymotion المرونة مع حزمة تبدأ من 0.50 دولارًا للساعة والجهاز. تتوفر نسخة تجريبية مجانية مدتها 30 يومًا لاختبار الميزات والقدرات.

PrimeOS



يوفر محاكي PrimeOS تجربة كاملة لسطح المكتب مثل نظام التشغيل Mac OS أو Windows مع إمكانية الوصول إلى العديد من تطبيقات Android. تم تصميم محاكي Android هذا ليوفر لك كلا العالمين - وهو مزيج كامل من Android والكمبيوتر الشخصي. يوفر PrimeOS دعم ARM ويعرض حالة البطارية، ويمزج مرونة Android مع وظائف الكمبيوتر.

يعد PrimeOS نظامًا أساسيًا قويًا متوفرًا لنظام التشغيل Windows 7 64 بت أو الإصدارات الأحدث، ويوفر مهام متعددة سلسة وتوافقًا مع تطبيقات Android.

يعتبر محاكي رائع للطلاب، حيث يتيح إدارة الأجهزة وأمانها بشكل محسّن.

يتيح لك نظام التشغيل ممارسة الألعاب الشهيرة مثل Call of Duty وFIFA ولكنه يتطلب ما لا يقل عن 4 جيجابايت من ذاكرة الوصول العشوائي وNvidia GeForce GTX 1060 أو AMD Radeon RX 580. وهو يعمل على Android 7 أو Android 11 أو أعلى.

المواصفات

- دعم التمهيد المزدوج بنقرة واحدة مع مثبت PrimeOS.
- يجمع بين نظام Android البيئي وواجهة النظام لتوفير تجربة لعب رائعة.
- يقدم أداءً عاليًا مقارنةً بنظام ذو السعر الرخيص Windows.
- يوفر دعم العملاء عبر البريد الإلكتروني والهاتف والدردشة ونموذج الاتصال
- المنصات المدعومة: Windows

الإيجابيات

- يدعم نوافذ متعددة
- يحتوي على واجهة مستخدم جميلة
- يعمل مباشرة على الأجهزة ويعمل كنظام تشغيل منفصل
- تشغيل ألعاب الأندرويد على جهاز الكمبيوتر الخاص بك
- أداة رسم الخرائط الرئيسية ستعمل على تحسين الأداء

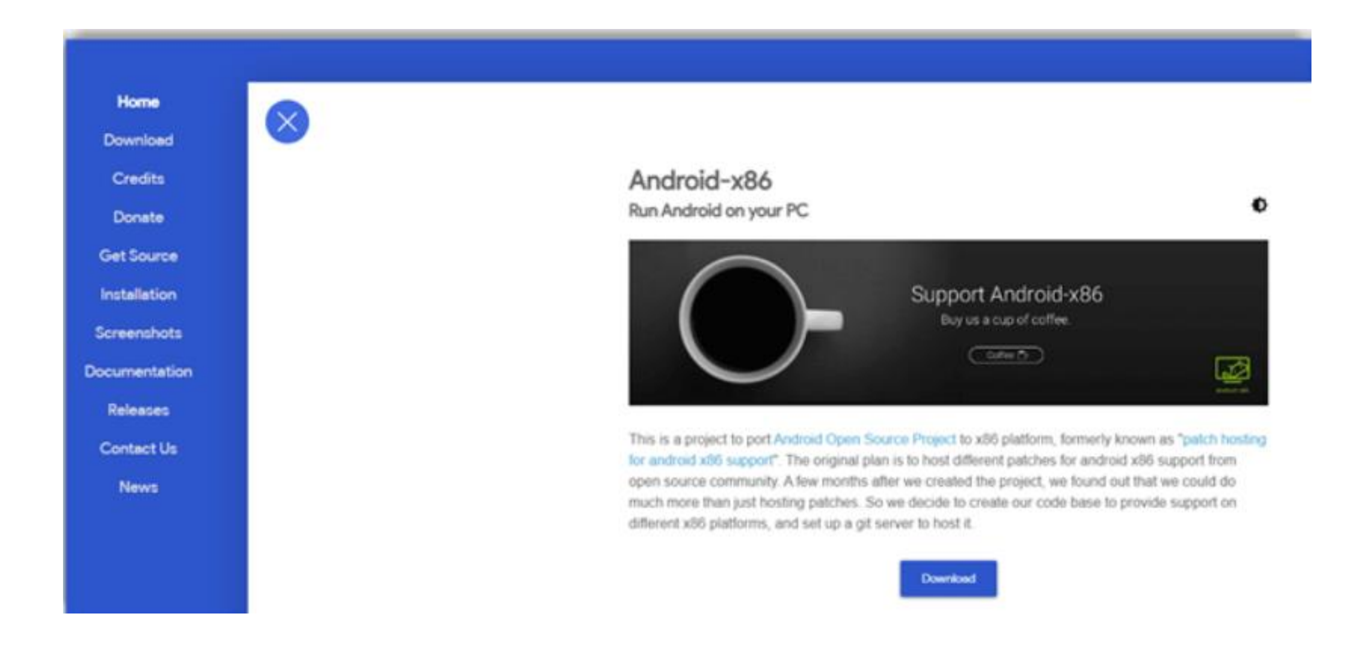
السلبيات

- عدد من الإعلانات
- لا يوجد تثبيت بنقرة واحدة
- دعم ملء الشاشة غير متوفر

السعر

- PrimeOS عبارة عن منصة مستقلة تقدم نسخة تجريبية مجانية مدى الحياة، مما يتيح للعملاء والمستقلين التواصل والتعاون وإكمال المشاريع المختلفة بكفاءة.

Android-x86



Android X86 عبارة عن منصة مفتوحة المصدر. هذا محاكي مفتوح المصدر ومرخص بموجب ترخيص Apache Public License 2.0. Android-x86: يدعم حالة البطارية واللمس المتعدد وARM. أداة متعددة الاستخدامات لتجربة جهاز الكمبيوتر الذي يعمل بنظام Android.

يتيح لك Android-x86 الاستمتاع بتجربة Android القوية على جهاز الكمبيوتر الذي يعمل بنظام التشغيل Windows 7 أو إصدار أحدث 64 بت. ومع دعم شبكة WiFi مع واجهة المستخدم الرسومية ومؤشر الماوس البرمجي والصوت (ALSA) وكاميرا V4l2، فإنه يضمن تغطية احتياجات الاتصال والوسائط الخاصة بك. يتضمن الحد الأدنى من المتطلبات VT-x أو AMD-V وذاكرة الوصول العشوائي (RAM) سعة 2 جيجابايت. يعمل بنظام التشغيل Android 10، وهو مثالي للعب الألعاب الشهيرة مثل Blackjack. ضع في اعتبارك أن الدقة الأصلية لجهاز netbook ووضع المرآة على الشاشات الخارجية وتقنية Bluetooth مدعومة أيضًا.

المواصفات

- توفير دعم WiFi مع واجهة المستخدم الرسومية.
- تعليق/استئناف الطاقة (وضع S3)
- دعم الكاميرا V4l2
- يقدم الدعم للدقة الأصلية لـ netbook
- يسمح بوضع المرآة على الشاشات الخارجية
- دعم التثبيت التلقائي للتخزين الخارجي
- دعم لوحة المفاتيح الخارجية
- يوفر دعم العملاء عبر البريد الإلكتروني
- دعم اللمس المتعدد: نعم

الإيجابيات

- يوفر دعمًا مستقرًا للأجهزة
- تقديم أداء عالي
- سهلة الاستخدام
- استخدام نظام تشغيل مفتوح المصدر

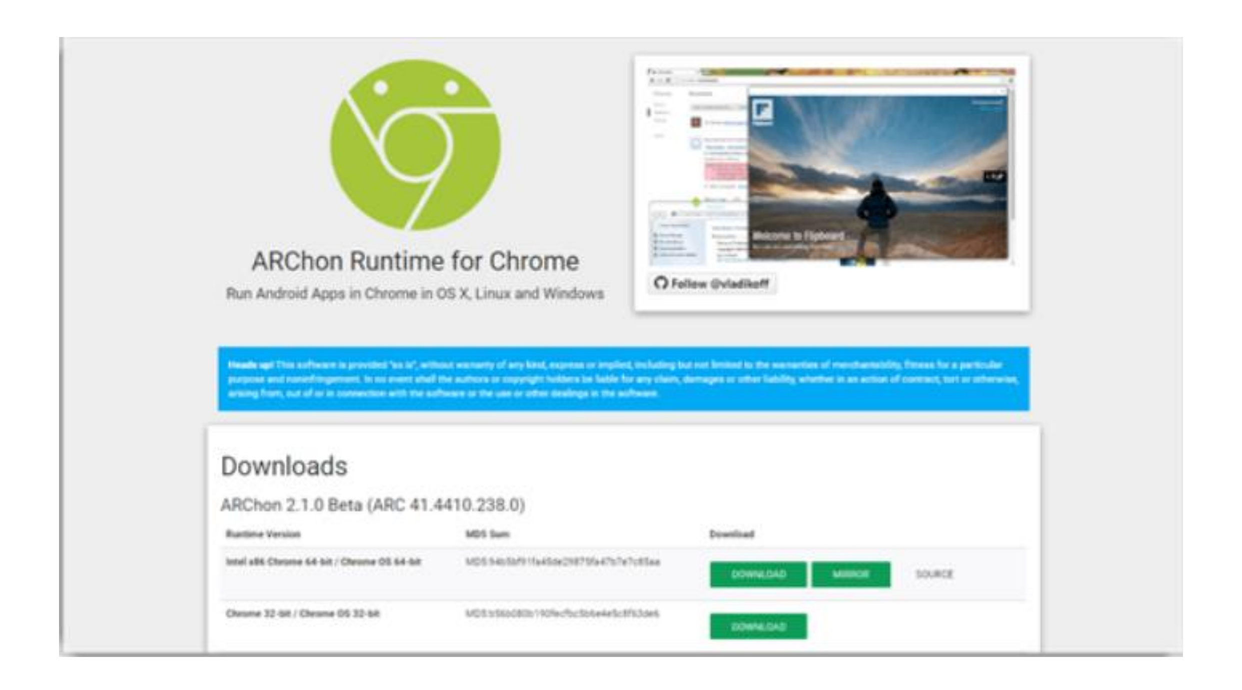
السلبيات

- الأداء بطيء

السعر

- Android-x86: مشروع مجاني مفتوح المصدر يتيح للمستخدمين تشغيل Android على أجهزة الكمبيوتر الشخصية، مما يوفر خيارًا فعالاً من حيث التكلفة لمحاكاة Android.

ARChon



يعتبر هذا التطبيق هو التطبيق الرسمي من جوجل لحزمة Chrome.

يتمتع هذا المحاكي المبسط بالقدرة على تشغيل أي تطبيق Android كتطبيق ChromeOS.

يعد ARChon أحد أفضل محاكيات Linux Android، ويدعم أحدث أنظمة Android، وهو متاح لنظام التشغيل Chrome. فهو يتيح لك تشغيل جميع التطبيقات وألعاب Android على Intel x86 Chrome 64 بت مع ذاكرة الوصول العشوائي (RAM) سعة 2 جيجابايت، مما يضمن تجربة سلسة أثناء التشغيل على Android 2.1 أو أعلى.

المواصفات

- خفيف الوزن للغاية لأنه مدمج مع Google Chrome
- يمكنك استخدامه مع جميع أنظمة التشغيل
- يوفر دعم العملاء عبر Reddit Community وARCHon Issue Tracker
- المنصات المدعومة: Linux و Windows

الإيجابيات

- يدعم أيضًا ARM
- تم دمجه في Chrome
- إنه خفيف الوزن ومفتوح المصدر
- إنه جيد للتطبيقات التي تجعل الإنتاجية أسهل

السلبيات

- الحد الأدنى من دعم المطور
- لا يتم تحديثه بشكل منتظم

السعر

- مجاني، وهو مشروع مفتوح المصدر متاح للتنزيل بسهولة، مما يتيح للمستخدمين تشغيل تطبيقات Android على متصفحات Chrome بكفاءة.

Ko Player



Ko player هي أداة محاكية لنظام Android تساعد المستخدمين على اكتساب تجربة لعب Android عالية الجودة على أجهزة الكمبيوتر الشخصية التي تعمل بنظام Windows أو Mac. ينصب التركيز الرئيسي لهذا المحاكي على توفير تجربة ألعاب خالية من التأخير لمستخدميه.

يعد Ko Player أحد أفضل محاكيات Android لنظام التشغيل Windows 7 والإصدارات الأحدث، وهو رائع للعب الألعاب الشهيرة مثل Call of Duty وSubway Surfers. فهو يسمح لك باستخدام لوحة الألعاب ولوحة المفاتيح والأجهزة الطرفية الأخرى، مما يضمن تجربة ألعاب غامرة. مع الحد الأدنى من متطلبات النظام لوحدة المعالجة المركزية AMD أو Intel ثنائية النواة وذاكرة الوصول العشوائي (RAM) سعة 2 جيجابايت، يعمل على نظام Android 4 أو أعلى. تأكد من حصولك على مواصفات النظام هذه على الأقل للاستمتاع بجميع ميزاته بسلاسة.

المواصفات

- يتيح لك الاستفادة من جميع ميزات ووظائف Android دون امتلاك أي جهاز
- يتمتع Ko player بواجهة مستخدم بسيطة وسهلة الاستخدام وتفاعلية
- يتيح لك تسجيل الفيديو المدمج تسجيل مقاطع الفيديو المفضلة لديك والاستمتاع بها في الوقت المناسب لك
- يتيح لك محاكي تطبيقات Android هذا أيضًا تسجيل مقاطع الفيديو
- تعزيز أداء الألعاب
- يمكنك تسجيل ومشاركة طريقة لعبك مع أصدقائك أو أي شخص تريده
- يأتي مزودًا بمتجر Google Play Store، مما يتيح لك الوصول إلى أي تطبيق تريده
- يوفر دعم العملاء عبر البريد الإلكتروني
- الأنظمة الأساسية المدعومة: Windows، Mac

الإيجابيات

- واجهة مستخدم سهلة الاستخدام وسهلة الإعداد
- يمكنك من تسجيل مقاطع الفيديو أيضًا
- الوصول الكامل إلى متجر Play

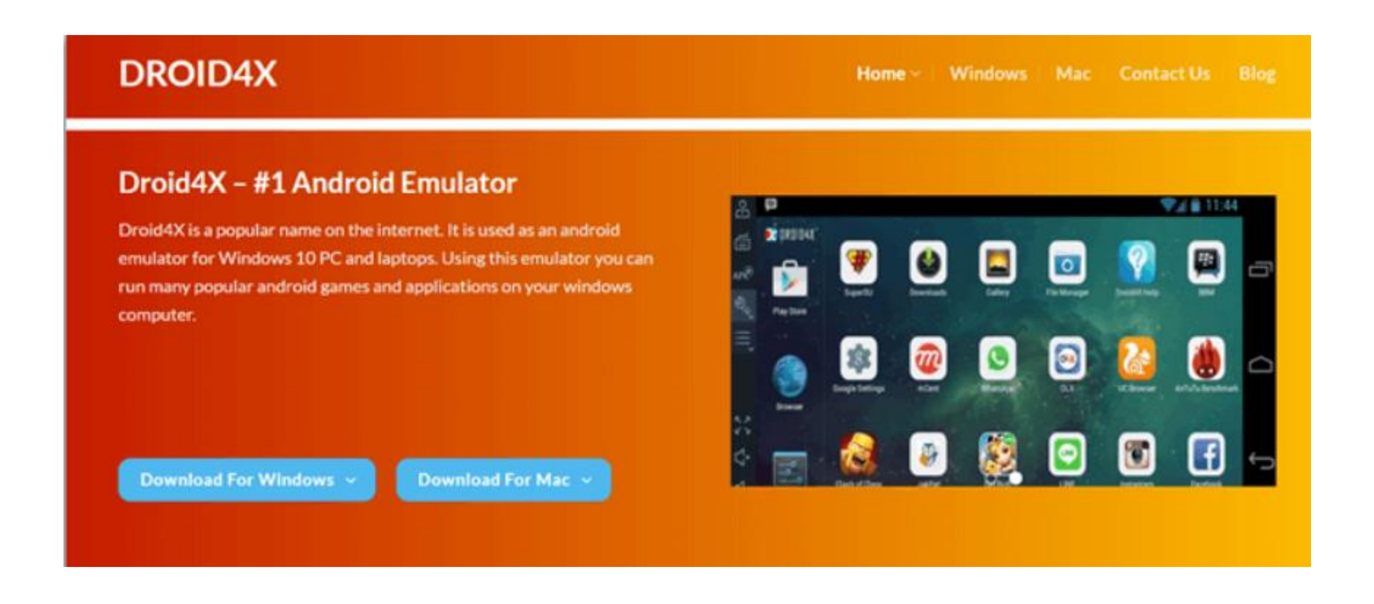
السلبيات

- لا توجد خيارات التخصيص لسهولة الاستخدام

السعر

- هو محاكي Android مجاني يقدم نسخة تجريبية مجانية مدى الحياة. فهو يتيح تجربة ألعاب وتطبيقات سلسة على سطح المكتب الخاص بك.

Droid4x



هو محاكي Android تم تطويره لأجهزة الكمبيوتر التي تعمل بنظام Windows والذي يسمح لك بتشغيل تطبيقات وألعاب الهاتف المحمول على سطح المكتب. يدعم هذا المحاكي معظم الألعاب المتوفرة في متجر الألعاب.

هو محاكي متعدد الاستخدامات، مثالي للعب ألعاب Android الشهيرة مثل Clash of Clans وSubway Surfers على أنظمة التشغيل Windows XP إلى 10. يتيح لك تخصيص عناصر التحكم وتنزيل التطبيقات التي تعمل على Android 4.2 أو أعلى مباشرة. مع الحاجة إلى ذاكرة وصول عشوائي سعة 2 جيجابايت فقط، يقوم Droid4x بتحويل جهاز الكمبيوتر الخاص بك إلى مركز قوي للألعاب بكفاءة.

المواصفات

- يساعدك على إكمال تجربة المستخدم على جهاز الكمبيوتر ويدعم شاشة الكمبيوتر التي تعمل باللمس للعمل عبر الأجهزة.
- يوفر محاكي Android لنظام التشغيل Windows 10 دعمًا للوحة المفاتيح ولوحة الألعاب للتكوين السريع للألعاب.
- يوفر التوافق والتنزيلات والمسجل والمطورين
- يوفر دعم العملاء عبر البريد الإلكتروني
- الأنظمة الأساسية المدعومة: Windows، Mac

الإيجابيات

- تشغيل الألعاب بسلاسة دون تأخير أو اختناق.
- يتم دعم تخصيص لوحة الألعاب ولوحة المفاتيح
- طريقة لعب رائعة مع شاشة لمس سريعة الاستجابة
- البرنامج آمن تمامًا وهو أمن لأجهزتك

السلبيات

- مستشعر الجيروسكوب لا يعمل
- لا يدعم البرمجيات المصغرة

السعر

- هو محاكي قوي يقدم نسخة تجريبية مجانية مدى الحياة، مما يتيح للمستخدمين تشغيل تطبيقات Android بسلاسة على أجهزة الكمبيوتر، مما يعزز تجربة المستخدم.

الأسئلة المتكررة

ما هو محاكي Android؟

محاكي Android هو تطبيق برمجي يسمح لهاتفك المحمول بتقليد ميزات نظام التشغيل Android على جهاز الكمبيوتر الخاص بك. يسمح لك بتثبيت تطبيقات Android على جهاز الكمبيوتر أو الكمبيوتر المحمول الخاص بك واستخدامها محليًا. يتم استخدامه بشكل رئيسي لأغراض التصحيح.

ما هو أفضل محاكي Android للكمبيوتر؟

فيما يلي بعض من أفضل محاكيات Android للكمبيوتر الشخصي:

BlueStacks – الأفضل للسحابة الهجينة أو أجهزة الكمبيوتر المحلية

LDPlayer – الأفضل للاعبين مثل Free Fire وPubG وCoC

NoxPlayer

ميمو

جينيموشن

PrimeOS

أندرويد-x86

ما هي فوائد استخدام برنامج Android Emulator؟

فيما يلي بعض الأسباب الأخرى لاستخدام محاكي Android:

سيكون له شاشة أكبر وبالتالي يوفر أيضًا عناصر تحكم أفضل لاستخدام التطبيقات في أجهزة الكمبيوتر.

لا تحتاج إلى الاهتمام بعمر بطارية أجهزة Android الخاصة بك.

تعد أجهزة الكمبيوتر الشخصية أقوى بشكل كبير من أجهزة Android بحيث يمكنها التعامل مع الألعاب ومقاطع الفيديو عالية الدقة بسرعة مناسبة.

كيف يعمل محاكي الأندرويد؟

تعمل محاكيات Android على مبدأ المحاكاة الافتراضية للنظام الأساسي لكل من الأجهزة والبرامج. يساعدك مدير AVD (جهاز Android الإفتراضي) على إعداد وإجراء التكوينات لأجهزة Android الافتراضية.

مع تحيات إخواكم في جيش الملاحم الإلكتروني

و

مجلس التعاون الإعلامي الإسلامي

ننصح بمراجعة كتاب الحرب الإلكترونية الجزء الأول – الأمن السيبراني –

من إعداد مجلس التعاون الإعلامي الإسلامي

دراسات سابقة صادرة عن جيش الملاحم الإلكتروني ومجلس التعاون الإعلامي الإسلامي

- أفضل خدمات VPN 2023
- ما هو أفضل تطبيق آمن للمراسلة



أفضل برامج مكافحة الفيروسات لعام 2023
إعداد: مجلس التعاون الإعلامي الإسلامي
تقديم: جيش الملاحم الإلكتروني
جيش الملاحم الإلكتروني
Al-Malahem Electronic Army

بسم الله الرحمن الرحيم

جيش الملاحم الإلكتروني

يقدم

*** دراسة ملحقة: أفضل برامج مكافحة الفيروسات لعام 2023 ***

إعداد

مجلس التعاون الإعلامي الإسلامي

Islamic Media Cooperation Council (IMCC)

4/ 1445هـ - 11/ 2023 م

المصدر

https://www.pcmag.com/picks/the-best-antivirus-protection

المقدمة

بدون برامج مكافحة الفيروسات، ستكون معلوماتك الشخصية وبياناتك وحتى حسابك البنكي في خطر. لقد اختبرنا أكثر من 40 أداة لمساعدتك في اختيار أفضل برامج مكافحة الفيروسات التي تناسب احتياجاتك.

هناك برودة في الهواء، وأوراق الأشجار تتحول إلى اللون الاصفر. البعض منا سيرى الثلج قريبا. بينما تجلس بجوار جهاز الكمبيوتر الدافئ الخاص بك، فكر في إبقائه مريحًا أيضًا. هل يرتجف في أعقاب سرقة البيانات التي تغذيها طروادة؟ هل تم تجميده بواسطة هجوم برامج الفدية؟ عندما يكون الطقس عالقًا في الداخل، فهذا هو الوقت المناسب للتحقق من حالة برنامج مكافحة الفيروسات لديك. تأكد من تحديثه. تأكد من تثبيت برنامج مكافحة الفيروسات، في هذا الشأن. إذا لم يكن الأمر كذلك، فهذا هو الوقت المناسب للحصول على الحماية.

ولكن ما هو برنامج مكافحة الفيروسات الذي يجب عليك اختياره؟ لقد قمنا بمراجعة أكثر من 40 أداة مساعدة لمكافحة الفيروسات، لذا يمكنك بسهولة اختيار الأداة التي تناسب احتياجاتك. لقد قمنا بتجميع أفضل 10 أدوات لمكافحة الفيروسات التي تم اختبارها، بالإضافة إلى ما يجب البحث عنه عند اختيار برنامج مكافحة الفيروسات المناسب لك، والذي يمكنك العثور عليه بعد القوائم أدناه.

الغوص بشكل أعمق: أفضل اختياراتنا التي تم اختبارها.

البرنامج	الرابط
Bitdefender — Bitdefender Antivirus Plus — Best Overall	https://www.bitdefender.com
norton — Norton AntiVirus Plus — Best for Antivirus From a Well-Known Brand	https://www.norton.com
eset — ESET NOD32 Antivirus — Best for Techies	https://www.eset.com
GDATA TRUST IN GERMAN SICHERHEIT — G Data Antivirus — Best Breadth of Features	https://www.gdatasoftware.com
Malwarebytes — Malwarebytes Premium — Best for Speedy Scans	https://www.malwarebytes.com
McAfee — McAfee AntiVirus — Best for One-PC Households	https://www.mcafee.com
SOPHOS HOME — Sophos Home Premium — Best for Thrifty Users	https://home.sophos.com/en-us
WEBROOT by opentext — Webroot AntiVirus — Best for a Small Footprint	https://www.webroot.com
total defense — Total Defense Essential Anti-Virus — Best for No-Frills Protection	https://www.totaldefense.com
TREND MICRO — Trend Micro Antivirus+ Security — Best for Single-PC Protection	https://www.trendmicro.com

Bitdefender Antivirus Plus

الأفضل بصورة عامة



لماذا اخترناه؟

يمكنك شراء أداة لمكافحة الفيروسات تقوم بكل ما ينبغي أن يقوم به برنامج مكافحة الفيروسات، أو يمكنك شراء أداة تقوم بالمزيد — أكثر بكثير. سيكون ذلك برنامج Bitdefender Antivirus Plus.

يمثل Plus في هذه الحالة العديد من الميزات. الحماية من برامج الفدية، ومتصفح قوي لمعاملاتك المالية، وحماية VPN لاتصالاتك، وهي ميزة تعمل على القضاء على متتبعي الإعلانات، والكشف التلقائي عن تصحيحات الأمان المفقودة، ومدير كلمات مرور بسيط... والقائمة تطول. على الرغم من أن اسمه يشير إلى برنامج مكافحة الفيروسات، إلا أن قائمة ميزات هذا البرنامج تتفوق على العديد من مجموعات الأمان.

ليس هذا فحسب، بل إنه أيضًا مضاد فيروسات جيد. تمنحها مختبرات الاختبار المستقلة بشكل روتيني درجات مثالية أو شبه مثالية، كما أنها تتفوق في العديد من اختباراتنا العملية.

أثبت نظام الدفاع الخاص ببرامج الفدية الخاصة به نفسه أثناء الاختبار أيضًا. وتعني ميزة الطيار الآلي أن كل هذا يحدث بأقل قدر من الإزعاج بالنسبة لك، كمستخدم.

هناك عدد قليل من المشاكل الصغيرة. على سبيل المثال، لا يتمتع مدير كلمات المرور بجميع الميزات الرائعة. وإذا كنت تريد استخدامًا غير محدود لشبكة VPN، فيجب عليك دفع مبلغ إضافي قليلًا. لكن، بشكل عام، يعد هذا خيارًا رائعًا للحماية من الفيروسات.

من يفضل ان يستعمله؟

إذا كنت تريد حماية شاملة مع القليل من التفاعل، فما عليك سوى تشغيل Bitdefender Antivirus Plus وتشغيل Autopilot الخاص به. الآن يمكنك الجلوس والقيام بأي شيء تريده!

الإيجابيات	السلبيات
درجات متميزة في الاختبارات المعملية المستقلة واختبارات الحماية من التصيد الاحتيالي	يسجل كميات نقل البيانات **(عيب خطير، ليس الأفضل للخصوصية)**
حماية متعددة الطبقات من برامج الفدية	يتطلب الوصول غير المحدود إلى VPN اشتراكًا منفصلاً
متصفح معزول للسلامة المصرفية نشط لا تتبع	الفحص الكامل الأول بطيء بشكل ملحوظ
يقدم VPN	
العديد من الميزات الإضافية التي تركز على الأمان	

Norton Antivirus Plus

أفضل برامج مكافحة الفيروسات من علامة تجارية مشهورة



Norton AntiVirus Plus

Best for Antivirus From a Well-Known Brand



4.5 Outstanding

لماذا اخترناه؟

بسرعة، قم بتسمية ثلاث شركات لمكافحة الفيروسات. هل كان نورتون واحدًا منهم؟ من المحتمل أنه منها.

لقد تطورت براعة Norton في مكافحة الفيروسات على مدار عقود من الزمن، ويعتبر Norton Antivirus Plus قمة هذا التطور. فهو يحصل على درجات ممتازة من المعامل المستقلة ويتفوق في العديد من اختباراتنا العملية، بما في ذلك اختبار باستخدام عشرات عينات برامج الفدية الحقيقية.

هناك ما هو أكثر في هذا البرنامج من مجرد برنامج مكافحة الفيروسات أيضًا.

يحمي جدار الحماية الخاص به من الهجمات الخارجية والخيانة من الداخل دون قصف المستخدم المطمئن باستعلامات منبثقة مربكة.

تعمل وحدة منفصلة على تعزيز حماية جدار الحماية من خلال اكتشاف هجمات الاستغلال وحظرها. تشتمل الميزات الإضافية الأخرى على نظام نسخ احتياطي يمكنه أرشفة ملفاتك محليًا أو في وحدة التخزين المتوفرة عبر الإنترنت، ومرشح البريد العشوائي لأولئك الذين ما زالوا بحاجة إلى مثل هذا الشيء، وأداة تحديث البرامج، والمزيد.

في وقت ما، كان Norton عبارة عن أفضل برنامج حماية لجهاز واحد، يحمي نظام Windows واحد فقط. يمكنك الآن الحصول على اشتراك لخمسة أجهزة لحماية أجهزة Windows وmacOS وAndroid وiOS. وهذا يجعل هذا التطبيق أكثر جاذبية.

من يفضل ان يستعمله؟

لقد ظلت تقنية Norton تحارب الفيروسات والبرامج الضارة الأخرى على مر العصور، ويعود تاريخها إلى أيام MS-DOS. إذا كنت تريد الحماية موفره من قبل علامة تجارية معروفة أنشأت منتجاتها على مدار عقود من الزمن، فإن Norton Antivirus Plus هو ما تحتاجه تمامًا.

الإيجابيات	السلبيات
درجات ممتازة في الاختبارات المعملية المستقلة	مكلفة نسبيا
حامي البيانات يحبط هجمات برامج الفدية	
تمكين النسخ الاحتياطي عبر الإنترنت	
يقدم VPN	
جدار الحماية ذكي	
يتضمن فحص الثغرات الأمنية وميزات أخرى على مستوى الجناح	

ESET NOD32 Antivirus

الأفضل للتقنيين



ESET NOD32 Antivirus

Best for Techies

●●●●○ 4.0 Excellent

لماذا اخترناه؟

عندما ترى التميمة سايبورغ ذات العيون الزرقاء من ESET تحدق بهدوء من شاشة ESET NOD32 Antivirus، فأنت تعلم أنك حصلت على بعض الحماية عالية التقنية. لقد حقق أعلى الدرجات في بعض الاختبارات المعملية المستقلة وبعض اختباراتنا الخاصة، ونحن نرغب دائمًا في رؤية كليهما. يتفوق ESET على العديد من المنافسين بميزات غير عادية عالية التقنية مثل فحص UEFI (واجهة البرامج الثابتة القابلة للتوسيع)، وهو أعلى من فحص قطاع التمهيد الأكثر شيوعًا. حتى أنه يبحث عن عمليات التطفل في قاعدة بيانات WMI (Windows Management Instrumentation).

نعم، أنت بحاجة إلى بعض الخبرة الفنية لفهم هذه الميزات عالية التقنية والاستفادة منها. وينطبق الشيء نفسه على نظام منع اختراق المضيف (HIPS)، الذي يهدف إلى اكتشاف ومنع الهجمات التي تحاول الاستفادة من نقاط الضعف في نظام التشغيل أو في البرامج الشائعة.

أما بالنسبة لنظام التحكم بالجهاز، فهو حلم التقنيين. يمكنك ممارسة التحكم الكامل في جميع أنواع الأجهزة الخارجية والأجهزة الفردية.

على سبيل المثال، يمكنك حظر محركات أقراص USB حتى لا يجلب الأطفال برامج ضارة إلى المنزل مع واجباتهم المدرسية، ولكن يسمح لهم على وجه التحديد بالأجهزة التي قمت بفحصها بنفسك.

على مستوى الجهاز أو النوع، يمكنك حظر جميع الاستخدامات، أو فرض الوصول للقراءة فقط، أو مجرد عرض تحذير.

من يفضل ان يستعمله؟

تبذل بعض أدوات مكافحة الفيروسات قصارى جهدها للعمل في الخلفية دون أي تدخل فني من قبل المستخدم. هذا ليس ESET NOD32 Antivirus. يعد برنامج مكافحة الفيروسات هذا مثاليًا لأولئك الذين يريدون أن يقوموا بدور نشط في الحماية الأمنية على الإنترنت. إذا كانت لديك المعرفة والمهارات اللازمة لاستخدامها، فإن ESET لديها الميزات المناسبة لك.

الإيجابيات	السلبيات
بعض الدرجات الممتازة من المعامل المستقلة	نتيجة ضعيفة في اختبارنا العملي لحظر البرامج الضارة
بعض الدرجات الجيدة في اختباراتنا العملية	التحكم في الجهاز معقد للغاية بالنسبة لمعظم المستخدمين
يستغل كتل مكون HIPS	الحماية من برامج الفدية غير فعالة في الاختبار
التحكم الشامل بالجهاز	

G Data Antivirus

أفضل مدى من الميزات



G Data Antivirus

Best Breadth of Features

4.0 Excellent

لماذا اخترناه؟

يشير موقع G Data على الويب إلى أن G Data أصدرت أول برنامج مضاد للفيروسات في عام 1985. وسواء كان البرنامج الأول أم لا، فإن G Data Antivirus يتمتع بتاريخ طويل وحافل.

عادةً ما يقوم اثنان من المختبرات الأربعة المستقلة التي نتبعها بتضمين هذه الأداة الجليلة في اختباراتهم. يمنحه AV-Test بشكل روتيني أعلى تصنيف ممكن، بينما تتراوح درجاته في اختبارات AV-Comparatives من النجاح إلى الكمال. حصلت G Data على درجات قريبة من الحد الأقصى في اختبارات الحماية العملية من البرامج الضارة واختبارات الدفاع عن التنزيلات الضارة.

طوال تطورها، حصلت أداة مكافحة الفيروسات هذه على العديد من أدوات الأمان الإضافية. مع تعطيل برنامج مكافحة الفيروسات العادي، اكتشفت طبقات الحماية من برامج الفدية المستندة إلى السلوك نصف العينات التي ألقيناها عليه.

سجل مكون اكتشاف الاستغلال نتائج أفضل من معظم المنافسين في الاختبار.

تشمل الميزات الإضافية الأخرى تصفية البريد العشوائي، وحماية BankGuard للمعاملات المالية، والدفاع النشط ضد برامج تسجيل لوحة المفاتيح، والتحكم الدقيق في برامج بدء التشغيل.

من يفضل ان يستعمله؟

يميل بعض الأشخاص نحو أحدث وأروع برامج الحماية من الفيروسات، بينما يفضل البعض الآخر برنامجًا ناضجًا يتمتع بمتسع من الوقت للتخلص من أي نقاط ضعف. G Data Antivirus عبارة عن أداة مساعدة متكاملة مع العديد من مكافآت الأمان. إنه الشيء المناسب لأولئك الذين يبحثون عن أداة مكافحة فيروسات قديمة.

الإيجابيات	السلبيات
درجة ممتازة في اختبارنا العملي للحماية من البرامج الضارة	درجات مختلفة في الاختبارات المعملية المستقلة
يحمي من أحصنة طروادة المصرفية، وبرامج تسجيل المفاتيح، وبرامج الفدية، والاستغلال	
يتضمن مرشح البريد العشوائي	

Malwarebytes Premium

الأفضل لإجراء عمليات المسح السريـع



Malwarebytes Premium

Best for Speedy Scans

●●●●○ 4.0 Excellent

لماذا اخترناه؟

لسنوات، كان برنامج Malwarebytes Free للتنظيف فقط هو الحل الأمثل عندما لا يتمكن برنامج مكافحة الفيروسات العادي من القيام بهذه المهمة، ولكنه كان دائمًا أداة متخصصة، وليس للاستخدام اليومي. من ناحية أخرى، يقدم Malwarebytes Premium جميع الميزات التي تتوقعها من برنامج مكافحة فيروسات واسع النطاق، بدءًا من الفحص حسب الطلب والجدول الزمني، بالإضافة إلى الوصول إلى الملفات.

يتميز الفحص الكامل بالسرعة ويستخدم العديد من تقنيات الحماية في الوقت الفعلي، بما في ذلك الكشف القائم على السلوك والكشف عن نشاط برامج الفدية والحماية من هجمات الاستغلال.

صحيح أن النتائج المعملية الخاصة ببرنامج Malwarebytes مختلطة، بعضها رائع وبعضها متوسط. وتؤكد الشركة أن تقنيات الكشف المتقدمة الخاصة بها ليست مناسبة تمامًا للاختبارات الموحدة. وفي اختباراتنا العملية، أثبت البرنامج فعاليته العالية، حيث حصل على 10 من 10 نقاط نادرة للحماية من البرامج الضارة ودرجات ممتازة للدفاع ضد صفحات الويب الضارة والاحتيالية.

من يفضل ان يستعمله؟

أي شخص يستخدم Malwarebytes Free لمعالجة خطأ أداة مكافحة فيروسات أخرى سيقدر برنامج Malwarebytes Premium ذو الإمكانات الكاملة. حتى لو لم تكن بحاجة أبدًا إلى هذا النوع من الإنقاذ، فإن الفحص السريع لهذا التطبيق ونتائج الاختبار العملي الممتازة يعدان بمثابة نقطة جذب كبيرة.

الإيجابيات	السلبيات
أعلى الدرجات في اختبارنا العملي للحماية من البرامج الضارة	لا توجد ميزات أكثر من مجرد برامج مكافحة الفيروسات الأساسية
حماية ممتازة ضد المواقع الخبيثة والاحتيالية	
درجات جيدة جدًا من المعامل المستقلة	

McAfee Antivirus

الأفضل للأسر التي لديها جهاز كمبيوتر واحد



McAfee AntiVirus

Best for One-PC Households

●●●●○ **4.0 Excellent**

لماذا اخترناه؟

لم يعد McAfee يوفر الحماية من الفيروسات عبر الأنظمة الأساسية التي يوفرها McAfee AntiVirus Plus، ولكن يعد McAfee AntiVirus الأساسي خيارًا قويًا لجهاز كمبيوتر واحد يعمل بنظام Windows.

تعد كلمة واحد كلمة مهمة هنا، حيث لا تجد الخصومات المعتادة على الحجم لثلاثة أو خمسة أو 10 تراخيص. يجب عليك شراء البرنامج مرة أخرى لكل جهاز جديد تريد حمايته.

تعشق المعامل المستقلة تقنية McAfee لمكافحة البرامج الضارة. ثلاثة من المختبرات الأربعة التي نتابعها تشمل McAfee في تحليلها، وتمنحها الثلاثة أقصى درجة ممكنة.

لقد حصل على درجات ممتازة في اختباراتنا العملية أيضًا. وهو يتجاوز ميزات مكافحة الفيروسات الأساسية من خلال نظام الحماية من برامج الفدية، وجدار الحماية البسيط، ونظام لإحباط عمليات التعدين الخفي، والمزيد.

من يفضل ان يستعمله؟

مع التحول من الحماية غير المحدودة على جميع الأنظمة الأساسية إلى تأمين جهاز كمبيوتر شخصي واحد يعمل بنظام Windows، يستقطب McAfee AntiVirus جمهورًا مختلفًا عن سابقه. ولكن هناك أشخاصًا يريدون فقط حماية هذا الكمبيوتر الشخصي المهم للغاية. إذا كنت واحدًا منهم، فيجب عليك إلقاء نظرة على McAfee.

الإيجابيات	السلبيات
درجات الاختبارات المعملية المثالية	غاب عن عينة واحدة من برامج الفدية التي تم تعديلها يدويًا
درجات ممتازة في اختباراتنا العملية	حماية لنظام التشغيل Windows فقط بدون خصم على الحجم
تعهد الحماية من الفيروسات	العديد من الميزات القديمة غائبة الآن

Sophos Home Premium

الأفضل للمستخدمين المقتصدين



Sophos Home Premium

Best for Thrifty Users

●●●●○ 4.0 Excellent

لماذا اخترناه؟

هو اسم كبير في مجال مكافحة الفيروسات على مستوى الأعمال، مع الإدارة عن بعد لإبقاء فريق تكنولوجيا المعلومات مسؤولاً عن الأمن. يقدم Sophos Home Premium نفس الإدارة عن بعد لك، أيها المستهلك.

يمكنك تثبيت برنامج الحماية من الفيروسات لعائلتك وأصدقائك، سواء كانوا في جميع أنحاء المدينة أو في جميع أنحاء البلاد، وإدارة جميع التثبيتات دون مغادرة مخبأك. وأفضل ما في الأمر أنه غير مكلف للغاية، حيث أن سعر 10 تراخيص يطابق ما يتقاضاه العديد من المنافسين مقابل ثلاثة تراخيص فقط.

يحتوي برنامج مكافحة الفيروسات هذا على نتيجة اختبار معملي واحدة حديثة فقط، ولكنها درجة جيدة — شهادة AAA من SE Labs. في اختبارنا العملي للحماية من البرامج الضارة، نجح في اكتشاف 100% وسجل 9.9 من أصل 10 نقاط محتملة.

كما حصل أيضًا على 100% للدفاع ضد صفحات الويب التي تستضيف البرامج الضارة. لكن حمايتها لا تتوقف عند هذا الحد. يحتوي برنامج الوكيل المحلي الصغير الخاص به على حماية فعالة من برامج الفدية، والدفاع ضد هجمات الاستغلال، ومرشح محتوى الرقابة الأبوية الأقل فعالية، وحماية معاملاتك المالية، ومنع اختطاف كاميرا الويب، والمزيد.

كما ذكرنا سابقًا، يمكنك إدارة جميع عمليات التثبيت الخاصة بك من خلال وحدة تحكم مريحة عبر الإنترنت. وفي الآونة الأخيرة، قامت شركة Sophos بتوسيع إمكانية التحكم عن بعد لتشمل تطبيقات Android وiOS، مما يعني أنه يمكنك ممارسة صلاحيات التحكم عن بعد من أي مكان.

من يفضل ان يستعمله؟

هل أنت خبير الأمان الافتراضي لعائلتك الممتدة أو دائرة أصدقائك؟ هل سئمت من القيادة عبر المدينة لإنقاذ عمك الحبيب بعد أن نقر على شيء لا ينبغي أن يكون لديه؟ مع Sophos Home Premium، يمكنك الاعتناء بأصدقائك أينما كنت.

الإيجابيات	السلبيات
درجات ممتازة في بعض الاختبارات العملية	نتائج محدودة من مختبرات الاختبار
تطبيق مناسب لإدارة أمن الأجهزة المحمولة	الرقابة الأبوية وحماية كاميرا الويب محدودة
يحمي من برامج الفدية، وكلوغرز، والاستغلال	درجة اختبار التصيد الاحتيالي واطئة
يدير ما يصل إلى 10 أجهزة كمبيوتر شخصية أو أجهزة Mac عن بعد	تتطلب الميزات المتقدمة خبرة تقنية غير عادية
غير مكلفة	

Webroot Antivirus

الأفضل لترك بصمة صغيرة

Webroot AntiVirus

Best for a Small Footprint

●●●●○ 4.0 Excellent



لماذا اخترناه؟

بدون شك، يعد Webroot SecureAnywhere AntiVirus أصغر برنامج مكافحة فيروسات رأيناه. عندما كانت الأقراص المرنة قياسية، كان من الممكن احتواؤها على قرص واحد فقط.

يمكن أن يكون الحضور المحلي لـ Webroot صغيرًا لأن ذكائه موجود في السحابة. مثل معظم أدوات مكافحة الفيروسات، فهو يزيل البرامج الضارة المعروفة عند رؤيتها، لكن العناصر غير المعروفة تحظى بمعاملة خاصة. فهو يرسل تفاصيل حول أي برنامج غير معروف إلى السحابة ويسمح بتشغيل هذا البرنامج في فقاعة، مما يجعل أي تغييرات في النظام افتراضية حتى لا تصبح دائمة.

يمكن أن يستغرق التحليل السحابي بعض الوقت، ولكن إذا تم تحديد أن البرنامج ضار، فإن Webroot يمسح البرنامج نفسه ويتراجع عن أي تغييرات في النظام.

ومع ذلك، فإن اكتشاف الإجراء المتأخر هذا ليس مناسبًا لمعظم الاختبارات القياسية. تتوقع المختبرات في الغالب أن يتم تحديد برنامج مكافحة الفيروسات فورًا أو لا يتم تحديده على الإطلاق. إن وجود Webroot في التقارير المعملية متقطع، مع مجموعة واسعة من النتائج. ولكن في اختباراتنا العملية، فإنه يحصل بشكل روتيني على درجات ممتازة.

من يفضل ان يستعمله؟

تتطلب بعض ميزات Webroot المتقدمة خبرة أعلى من المتوسط، لذلك لا يضر إذا كنت خبيرًا أمنيًا لعائلتك أو دائرة أصدقائك. سواء كنت خبيرًا أم لا، فمن المؤكد أنك ستقدر حجمه الصغير وعمليات المسح فائقة السرعة.

الإيجابيات	السلبيات
مسح سريع، حجم صغير	لم يعد يقدم المراقبة والتكوين عن بعد
ضوء على موارد النظام	حماية غير كاملة ضد برامج الفدية المعدلة يدويًا
يمكنه معالجة أضرار برامج الفدية	نتائج الاختبارات المعملية محدودة
الخيارات المتقدمة	تتطلب الميزات المتقدمة خبرة غير عادية
	لا يوجد خصم على الحجم
	يمكن أن تكون إعدادات جدار الحماية مربكة

Total Defense Essential Antivirus

الأفضل للحماية بدون زخرفة



Total Defense Essential Anti-Virus

Best for No-Frills Protection

3.5 Good

لماذا اخترناه؟

تتضمن بعض تطبيقات مكافحة الفيروسات الكثير من برامج الأمان الإضافية التي تكاد تكون بمثابة مجموعات.

من ناحية أخرى، يلتزم برنامج Total Defense Essential Anti-Virus بالمهام الأساسية لأداة مكافحة الفيروسات: البحث عن البرامج الضارة عند الطلب، وفي الموعد المحدد، وعند الوصول إلى الملفات. كان وقت الفحص الكامل لـ Total Defense متوسطًا تقريبًا، لكن الفحص الثاني خفض 90% من ذلك بفضل التحسين.

حصلت Total Defense على أعلى الدرجات من مختبر اختبار AV-Comparatives في السنوات الماضية. تتراوح درجاتها الثلاثة الحالية من Advanced+ (الأفضل) إلى Standard.

لا يزال هذا أفضل من العديد من المنافسين الذين ليس لديهم أي نتائج مختبرية على الإطلاق. وفي اختباراتنا العملية، حصل البرنامج على درجات من جيد جدًا إلى ممتاز، وأثبت مهارة خاصة في اكتشاف مواقع الويب الضارة والاحتيالية والدفاع ضدها.

من يفضل ان يستعمله؟

يعد Total Defense Essential Anti-Virus خيارًا جيدًا إذا كنت تريد أداة مكافحة فيروسات سريعة وغير مكلفة تؤدي وظيفتها دون إثارة أي ضجة.

الإيجابيات	السلبيات
درجات اختبار ممتازة ضد المواقع الخبيثة والاحتيالية	نتائج اختبارات قليلة من مختبرات مستقلة
درجة جيدة جدًا في اختبار الحماية من البرامج الضارة العملي	
ضمان خلوه من الفيروسات	

Trend Micro Antivirus + Security

الأفضل لحماية جهاز كمبيوتر واحد



لماذا اخترناه؟

على الرغم من أنها نشأت في لوس أنجلوس، إلا أن Trend Micro أصبحت الآن شركة أمنية عالمية مقرها في اليابان، وقد استحوذت على العديد من الشركات الأمنية الأخرى على مر السنين.

إن تقنيتها الجماعية تجعل Trend Micro Antivirus+ Security أكثر من مجرد برنامج مكافحة فيروسات. ومن بين المكونات الأخرى، تتميز Trend Micro بميزة Pay Guard لحماية معاملاتك المالية؛ معزز جدار الحماية؛ تصفية البريد العشوائي باستخدام مكون منفصل لمكافحة الاحتيال؛ حماية متعددة الطبقات من برامج الفدية؛ كاشف للتعدين غير المصرح به للعملات المشفرة، وترميز الروابط الخطيرة في نتائج البحث ووسائل التواصل الاجتماعي.

ولكن هل يعمل؟ تختلف النتائج. لقد كرمت AV-Test شركة Trend Micro بشكل متكرر بحصولها على درجة ممتازة، على الرغم من انخفاضها في التقرير الأخير. لقد أثبتت التقييمات السابقة التي أجرتها SE Labs أنها على أعلى مستوى AAA. ومع ذلك، فقد فشلت في أحد الاختبارات الثلاثة التي أجرتها AV-Comparatives. كما أنها فشلت أيضًا في اختبارين صعبين أجرتهما MRG-Effitas. وعلى الجانب الإيجابي، فقد حصل على درجات ممتازة في اختباراتنا للدفاع ضد مواقع الويب الضارة والاحتيالية.

هذا برنامج مضاد فيروسات لجهاز واحد بدون تخفيضات في الحجم. إذا كنت تريد ترخيصًا متعدد الأجهزة من Trend Micro، فسيتعين عليك اختيار أحد برامجها.

من يفضل ان يستعمله؟

لا تلجأ إلى Trend Micro Antivirus+ Security لحماية منزل مليء بأجهزة الكمبيوتر. هذا ليس ما هو عليه. بدلاً من ذلك، قم بتثبيته على جهاز الكمبيوتر الأساسي الذي تقضي عليه ساعات العمل ووقت اللعب.

الإيجابيات	السلبيات
النتيجة المثالية في اختبار مكافحة التصيد لدينا	خضعنا للاختبار العملي للحماية من البرامج الضارة
درجة مثالية ضد صفحات استضافة البرامج الضارة	بعض حالات الفشل في الاختبارات المعملية المستقلة
الحماية من برامج الفدية ذات الطبقات	خيارات حماية الشبكة الاجتماعية مؤرخة
ملحق متصفح متعدد الأوجه	لا يوجد ترخيص جماعي متعدد الأجهزة
العديد من الميزات الإضافية	

الأسئلة الشائعة

دليل الشراء: أفضل برامج مكافحة الفيروسات لعام 2023

ما هي الفيروسات والبرامج الضارة وبرامج الفدية؟

نحن نسميه مضاد فيروسات، ولكن في الحقيقة، من غير المحتمل أن تصاب بفيروس كمبيوتر فعلي. تهدف البرامج الضارة هذه الأيام إلى كسب المال، ولا توجد طريقة سهلة للاستفادة من نشر الفيروس.

تعد برامج الفدية وأحصنة طروادة التي تقوم بسرقة البيانات أكثر شيوعًا، وكذلك الروبوتات التي تسمح لراعي الروبوتات بتأجير جهاز الكمبيوتر الخاص بك لأغراض شائنة. تتعامل أدوات مكافحة الفيروسات الحديثة مع أحصنة طروادة والجذور الخفية وبرامج التجسس وبرامج الإعلانات المتسللة وبرامج الفدية والمزيد.

كما ذكرنا، قام PCMag بمراجعة أكثر من 40 أداة مساعدة تجارية مختلفة لمكافحة الفيروسات، هذا بالإضافة الى العديد من أدوات مكافحة الفيروسات المجانية التي استعرضناها. لقد قمنا باختيار احد التطبيقات بين هذا المجال الواسع من تطبيقات مكافحة الفيروسات وأسميناه تطبيق اختيار المحررين، ثم قمنا بتكريم الآخرين بتقييمات أربع نجوم أو أفضل. إذا كان لديك برامج ضارة فيجب أن تعالج إحدى الأدوات المساعدة المدرجة في هذه المقالة المشكلة.

ماذا عن Windows Defender؟

توفر هذه التطبيقات التجارية حماية تتجاوز برامج مكافحة الفيروسات المضمنة في Windows. ومع ذلك، يبدو برنامج Microsoft Defender Antivirus أفضل في الآونة الأخيرة، مع بعض النتائج القوية من مختبرات الاختبار المستقلة. كان الجمع بين النتائج المعملية الجيدة والنتيجة الرائعة في اختبار الحماية من البرامج الضارة العملي كافيًا لرفع تصنيفه إلى 3.5 نجمة. وباعتبارها أداة مساعدة مجانية ومدمجة، فإننا لا نقوم بتضمينها في هذه الجولة من تطبيقات مكافحة الفيروسات التجارية.

نحن نستمع إلى مختبرات اختبار مكافحة الفيروسات

نحن نأخذ النتائج التي أبلغت عنها مختبرات اختبار مكافحة الفيروسات المستقلة على محمل الجد. الحقيقة البسيطة المتمثلة في ظهور برنامج مكافحة الفيروسات الخاص بالشركة في النتائج هي بمثابة تصويت بالثقة، من نوع ما. وهذا يعني أن المختبر اعتبر البرنامج مهمًا، وشعرت الشركة أن تكلفة الاختبار كانت جديرة بالاهتمام. وبطبيعة الحال، فإن الدرجات العالية في الاختبارات مهمة أيضًا.

نحن نتبع أربعة مختبرات تصدر تقارير تفصيلية بانتظام: SE Labs وAV-Test Institute وMRG-Effitas وAV-Comparatives. لقد ابتكرنا نظامًا لتجميع نتائجهم للحصول على تصنيف من 0 إلى 10.

كيف نختبر دفاعات البرامج الضارة وبرامج التجسس وبرامج الإعلانات المتسللة

نحن نخضع أيضًا كل تطبيق مضاد فيروسات لاختبارنا العملي للحماية من البرامج الضارة، وذلك جزئيًا للتعرف على كيفية عمل التطبيق. اعتمادًا على مدى دقة برنامج مكافحة الفيروسات في منع تثبيت البرامج الضارة، يمكنه الحصول على ما يصل إلى 10 نقاط للحماية من البرامج الضارة.

يستخدم اختبار الحماية من البرامج الضارة لدينا بالضرورة نفس مجموعة العينات لعدة أشهر. للتحقق من طريقة تعامل البرنامج مع البرامج الضارة الجديدة تمامًا، نقوم باختبار كل برنامج مكافحة فيروسات باستخدام مجموعة كبيرة من عناوين URL الجديدة تمامًا لاستضافة البرامج الضارة والتي توفرها MRG-Effitas، مع ملاحظة النسبة المئوية منها التي تم حظرها. تحصل التطبيقات على رصيد متساوٍ لمنع الوصول إلى عنوان URL الضار ولمسح البرامج الضارة أثناء التنزيل.

تحصل بعض التطبيقات على تقييمات ممتازة من المعامل المستقلة ولكنها لا تحقق نتائج جيدة في اختباراتنا العملية. في مثل هذه الحالات، نلجأ إلى المختبرات، لأنها توفر موارد أكبر بكثير لاختباراتها.

اريد معرفة المزيد؟ يمكنك البحث للحصول على وصف تفصيلي لكيفية اختبار برامج الأمان.

ما هو أفضل مضاد فيروسات للحماية من البرامج الضارة؟

تميز أدوات مكافحة الفيروسات نفسها من خلال تجاوز أساسيات الفحص عند الطلب والحماية من البرامج الضارة في الوقت الفعلي. تقوم بعض عناوين URL بتقييم عناوين URL التي تزورها أو التي تظهر في نتائج البحث باستخدام نظام ترميز الألوان باللون الأحمر والأصفر والأخضر. يحظر البعض بشكل فعال العمليات على نظامك من الاتصال بعناوين URL المعروفة لاستضافة البرامج الضارة أو بصفحات الاحتيال (التصيد الاحتيالي).

تحتوي جميع البرامج على عيوب، وفي بعض الأحيان تؤثر هذه العيوب على أمانك. يحافظ المستخدمون الحذرون على تصحيح نظام التشغيل Windows وجميع البرامج، وإصلاح تلك العيوب في أسرع وقت ممكن. يمكن لفحص الثغرات الأمنية الذي توفره بعض تطبيقات مكافحة الفيروسات التحقق من وجود جميع التصحيحات الضرورية وحتى تطبيق أي تصحيحات مفقودة.

تأتي برامج التجسس بأشكال عديدة، بدءًا من البرامج المخفية التي تسجل كل ضغطة تقوم بها على المفاتيح، وحتى أحصنة طروادة التي تتنكر في صورة برامج صالحة بينما تقوم بالتنقيب في بياناتك. يجب أن يتعامل أي برنامج مكافحة فيروسات مع برامج التجسس، جنبًا إلى جنب مع جميع أنواع البرامج الضارة الأخرى، ولكن بعضها يشتمل على مكونات متخصصة مخصصة للحماية من برامج التجسس.

تتوقع أن يقوم برنامج مكافحة الفيروسات بتحديد البرامج السيئة وإزالتها وترك البرامج الجيدة بمفردها. ماذا عن البرامج المجهولة، التي لا يستطيع AV الخاص بك تحديدها على أنها جيدة أو سيئة؟ من الناحية النظرية، يمكن للاكتشاف المعتمد على السلوك أن يحميك من البرامج الضارة، لذلك لم يوجهها الباحثون الجدد مطلقًا.

ومع ذلك، هذه ليست دائما خدمة خالصة. ليس من غير المألوف أن تقوم أنظمة الكشف السلوكي بالإبلاغ عن العديد من السلوكيات غير الضارة التي تقوم بها البرامج الشرعية.

تعد القائمة المسموح بها طريقة أخرى لحل مشكلة البرامج غير المعروفة. يسمح هذا النوع من أنظمة الأمان فقط بتشغيل البرامج الجيدة المعروفة. المجهولون ممنوعون لا يناسب هذا الوضع جميع المواقف، لكنه قد يكون مفيدًا.

يتيح Sandboxing تشغيل البرامج غير المعروفة، ولكنه يعزلها عن الوصول الكامل إلى نظامك، حتى لا تتمكن من إحداث ضرر دائم. تعمل هذه الطبقات المضافة المتنوعة على تعزيز الحماية ضد البرامج الضارة.

أين ذهب Kaspersky؟

تصدر برنامج Kaspersky Anti-Virus قوائم الاختبارات المعملية لمكافحة الفيروسات لسنوات عديدة، حيث حصل على درجات مثالية أو شبه مثالية. لقد حازت أيضًا على جائزة اختيار المحررين من PCMag لسنوات لا حصر لها. إنها جذابة وفعالة. ولم يعد يظهر في قائمتنا لأفضل تطبيقات مكافحة الفيروسات. هذا هو السبب:

لسنوات عديدة، واجهت شركة Kaspersky اتهامات وانتقادًا على أساس أصولها الروسية، على الرغم من أن أيًا من هذه الادعاءات لم تكن مدعومة بأدلة دامغة على السلوك الخبيث. نحن في PCMag نركز على إمكانيات التطبيقات، وليس على الضجة المحيطة بالشركة. ومع ذلك، فإن الحرب الحالية في أوكرانيا زادت من المخاطر. لقد قطعت الحكومات والأطراف الثالثة علاقاتها مع Kaspersky. صنفت لجنة الاتصالات الفيدرالية (FCC) برنامج Kaspersky على أنه خطر على الأمن القومي. وفي الآونة الأخيرة، منعت كندا استخدام Kaspersky على الأجهزة المملوكة للحكومة.

بعد دراسة الأمر، لم يعد بإمكاننا أن نوصيك بشراء برامج الأمان من Kaspersky. لقد تركنا التقييمات في مكانها، مع تحذير، لأنها توفر معلومات مفيدة. ولكننا، على الأقل في الوقت الحالي، نقوم بإزالة برامج Kaspersky من قوائم "الأفضل" لدينا.

ما هو أفضل برنامج مكافحة فيروسات للحماية من برامج الفدية وجدران الحماية؟

لا تعد جدران الحماية وتصفية البريد العشوائي من ميزات مكافحة الفيروسات الشائعة، ولكن بعض أفضل اختياراتنا تتضمنها كمكافآت. بعض برامج مكافحة الفيروسات هذه مليئة بالميزات أكثر من بعض مجموعات الأمان.

من بين الميزات الإضافية الأخرى التي ستجدها هي المتصفحات الآمنة للمعاملات المالية، والحذف الآمن للملفات الحساسة، ومسح آثار الكمبيوتر وسجل التصفح، ومراقبة الائتمان، ولوحات المفاتيح الافتراضية لإحباط برامج تسجيل المفاتيح، والحماية عبر الأنظمة الأساسية، والمزيد. وبطبيعة الحال، لقد ذكرنا بالفعل وضع الحماية، وفحص الثغرات الأمنية، والقائمة المسموح بها للتطبيقات.

نحن نرى المزيد والمزيد من تطبيقات مكافحة الفيروسات تضيف وحدات مصممة خصيصًا للحماية من برامج الفدية. يعمل بعضها عن طريق منع التغييرات غير المصرح بها على الملفات المحمية. ويراقب آخرون السلوكيات المشبوهة التي تشير إلى وجود برامج ضارة. بل إن البعض يهدف إلى عكس الضرر. ونظراً لنمو هذه الآفة، فإن أي حماية إضافية تكون مفيدة.

ما وراء برامج مكافحة الفيروسات: قم بتثبيت VPN

تعمل أداة مكافحة الفيروسات لديك في الخلفية لتفادي أي احتمال ضعيف للإصابة بالبرامج الضارة، ولكن قدراتها لا تتجاوز حدود جهاز الكمبيوتر الخاص بك. عندما تتصل بالإنترنت الجامح والغامض، فإنك تخاطر باحتمالية تعرض بياناتك للخطر أثناء النقل. يمكن أن يساعد الالتزام بمواقع HTTPS عندما يكون ذلك ممكنًا، ولكن للحصول على الحماية الكاملة لبياناتك أثناء النقل، يجب عليك تثبيت VPN (شبكة خاصة افتراضية). يعد هذا المكون مهمًا بدرجة كافية لدرجة أننا بدأنا نراه كميزة إضافية في بعض أدوات مكافحة الفيروسات.

ما هو أفضل برامج مكافحة الفيروسات؟

ما هي برامج مكافحة الفيروسات التي يجب عليك اختيارها؟ على الرغم من أن لديك ثروة من الخيارات، إلا أن هناك خيارين يبرزان عن الباقي. حصل برنامج Bitdefender Antivirus Plus على درجات ممتازة من ثلاثة مختبرات مستقلة لاختبار مكافحة الفيروسات، كما أنه يحتوي على ميزات أكثر من بعض مجموعات الأمان. يقدم Norton AntiVirus Plus أيضًا العديد من الميزات على مستوى المجموعة، ويحصل على درجات ممتازة من جميع مختبرات الاختبار الأربعة التي نتابعها. لقد قمنا بتسمية هذين الخيارين كخيار المحررين لبرامج مكافحة الفيروسات التجارية، لكنهما ليسا تطبيقي مكافحة الفيروسات الوحيدين اللذين يستحقان الاهتمام. اقرأ تقييمات برامجنا الأعلى تقييمًا، ثم اتخذ قرارك بنفسك.

جدول النتائج

- التقييم
- فحص البرامج الضارة عند الطلب
- فحص البرامج الضارة عند الوصول
- تصنيف الموقع
- حظر عناوين URL الضارة
- الحماية من التصيد
- الحماية المبنية على السلوك
- فحص الضعف
- جدار الحماية
- من أين يمكنك شراءه

The Best Antivirus Software for 2023

	Bitdefender	norton	eset	GDATA TRUST IN GERMAN SICHERHEIT	Malwarebytes	McA
Our Picks	Bitdefender Antivirus Plus Check Price	Norton AntiVirus Plus Check Price	ESET NOD32 Antivirus Check Price	G Data Antivirus See It $29.95 at G DATA Software	Malwarebytes Premium Check Price	McAfee Ant Check P
Editors' Rating	EDITORS' CHOICE 5.0 Editor Review	EDITORS' CHOICE 4.5 Editor Review	4.0 Editor Review	4.0 Editor Review	4.0 Editor Review	Editor Re
On-Demand Malware Scan	✓	✓	✓	✓	✓	✓
On-Access Malware Scan	✓	✓	✓	✓	✓	✓
Website Rating	✓	✓	✗	✗	✗	✓
Malicious URL Blocking	✓	✓	✓	✓	✓	✓
Phishing Protection	✓	✓	✓	✓	✓	✓
Behavior-Based Detection	✓	✓	✓	✓	✓	✓
Vulnerability Scan	✓	✓	✗	✗	✗	✓
Firewall	✗	✓	✗	✗	✗	✓
Where to Buy	$19.99 for 3 Devices Per Year at Bitdefender	$14.99 for 1-Device on 1-Year Plan at Norton LifeLock	$59.99 for 1 Device on 2 Year Plan at ESET $39.99 for 1 Device on 1 Year Plan at ESET	$29.95 at G DATA Software	$44.99 at Malwarebytes	$19.99 at McAfee

	ytes	McAfee	SOPHOS HOME	WEBROOT	total defense	TREND MICRO
Our Picks	tes e	McAfee AntiVirus Check Price	Sophos Home Premium Check Price	Webroot AntiVirus See It $19.99 for a Limited Time (50% Off 1-Year Plan) at Webroot	Total Defense Essential Anti-Virus See It $29.99/Month at Total Defense	Trend Micro Antivirus+ Security See It $29.95/Year at Trend Micro Small Business
Editors' Rating	.0 ew	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review	●●●●○ 4.0 Editor Review	●●●◐○ 3.5 Editor Review	●●●◐○ 3.5 Editor Review
On-Demand Malware Scan		✓	✓	✓	✓	✓
On-Access Malware Scan		✓	✓	✓	✓	✓
Website Rating		✓	✗	✓	✗	✓
Malicious URL Blocking		✓	✓	✓	✓	✓
Phishing Protection		✓	✓	✓	✓	✓
Behavior-Based Detection		✓	✓	✓	✓	✓
Vulnerability Scan		✓	✗	✗	✗	✗
Firewall		✓	✗	✓	✗	✗
Where to Buy	›	$19.99 at McAfee ›	$39.99 Per Year at Sophos ›	$19.99 for a Limited Time (50% Off 1-Year Plan) at Webroot ›	$29.99/Month at Total Defense ›	$29.95/Year at Trend Micro Small Business ›

مع تحيات إخواكم في جيش الملاحم الإلكتروني

و

مجلس التعاون الإعلامي الإسلامي

تتصح بمراجعة كتاب الحرب الإلكترونية الجزء الأول – الأمن السيبراني –

من إعداد مجلس التعاون الإعلامي الإسلامي

بالإضافة إلى الدراسات السابقة

- أفضل خدمات VPN 2023
- ما هو أفضل تطبيق آمن للمراسلة
- أفضل محاكيات Android